

Patrick Carey, (Bar No. 308623)
Mark Todzo, (Bar No. 168389)
LEXINGTON LAW GROUP, LLP
503 Divisadero Street
San Francisco, California 94105
Telephone: (415) 913-7800
pcarey@lexlawgroup.com
mtodzo@lexlawgroup.com

David S. Golub, (pro hac vice forthcoming)
Steven Bloch, (pro hac vice forthcoming)
Ian W. Sloss, (pro hac vice forthcoming)
Jennifer Sclar, (pro hac vice forthcoming)
John Serebinski, (pro hac vice forthcoming)
SILVER GOLUB & TEITELL LLP
One Landmark Square, 15th Floor
Stamford, Connecticut 06901
Telephone: (203) 325-4491
dgolub@sgtlaw.com

Attorneys for Plaintiffs and the Proposed Classes

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

A.A., a minor, by and through their guardian ad
litem, MARCELO MUTO; A.B., a minor, by and
through their guardian ad litem HEATHER
BRESSETTE; and A.C., a minor, by and through
their guardian ad litem DARRYL MAULTSBY,
individually and on behalf of all others similarly
situated,

Plaintiffs,

v.

BYTEDANCE INC; BYTEDANCE LTD;
TIKTOK LTD; TIKTOK INC; TIKTOK PTE.
LTD; and TIKTOK U.S. DATA SECURITY INC.,
Defendants.

Case No.

CLASS ACTION

COMPLAINT

DEMAND FOR JURY TRIAL

1 Minor Plaintiffs A.A., A.B., and A.C. (collectively, “Minor Plaintiffs” or “Plaintiffs”), by and
 2 through their respective guardians ad litem and their undersigned counsel, hereby allege the following
 3 against Defendants, on behalf of themselves and all others similarly situated, based on personal
 4 knowledge, information and belief, the investigation of counsel, and public sources.

5 **NATURE OF THE ACTION**

6 1. This action arises out of Defendants’ invasion of privacy and unfair business practices
 7 directed toward millions of children in the United States under the age of 13 in violation of the law and
 8 societal norms. Specifically, from March 1, 2019 through the present (the “Class Period”), Defendants
 9 have knowingly permitted and encouraged children under the age of 13 to create user accounts on the
 10 TikTok app for the purpose of collecting intimate, deeply intrusive data points about them and their on
 11 line behavior without notice and parental consent. Defendants use this unlawfully collected personal
 12 information for the purpose of providing personally curated content that will keep children engaged with
 13 TikTok, so that Defendants can serve them copious amounts of behavioral advertising and/or share their
 14 information with third parties. Defendants engaged in this unlawful behavior for one reason – profit.
 15 Indeed, children are so integral to Defendants’ profitability, Defendants were unwilling or unable to
 16 cease their unlawful business practices in the face of a Permanent Injunction and a Civil Penalty that
 17 they entered into with the United States Government on March 27, 2019, which prohibited Defendants
 18 from their continued collection and use of the personal information of children without verifiable
 19 parental consent.

20 2. Defendants Bytedance LTD, Bytedance, Inc.; TikTok LTD, TikTok Inc., TikTok PTE
 21 LTD, and TikTok U.S. Data Security Inc. (collectively, “TikTok”) operate one of the world’s largest
 22 social media platforms that reaches millions of Americans under the age of 13.

23 3. TikTok’s user base is disproportionately made up of children. From the outset,
 24 Defendants considered U.S. teens a “golden audience.”¹

25
 26
 27
 28 ¹ Paul Mozur, Chinese Tech Firms Forced to Choose Market: Home or Everywhere Else, N.Y. TIMES
 (August 9, 2016).

1 4. Defendants know that TikTok is an attractive social media destination for children.
2 Nonetheless, Defendants have a history of knowingly allowing children under 13 to create and use
3 TikTok accounts without their parents' knowledge or consent, have collected extensive data from those
4 children, and have failed to comply with parents' requests to delete their children's accounts and
5 personal information.

6 5. On February 27, 2019 the United States filed a Complaint against Musical.ly and
7 Musical.ly, Inc. alleging that defendants' were unlawfully collecting and using the personal information
8 of children in the operation of their free on line video-sharing app. *United States of America v.*
9 *Musical.ly et. al.*, No. 2:19-cv-1439 (C.D. Cal. Feb. 27, 2019) (Dkt. No. 1).

10 6. One month later, on March 27, 2019, Musical.ly and Musical.ly, Inc., (respectively
11 renamed TikTok Ltd. and TikTok Inc.in April 2019), entered into a Stipulated Order for Civil Penalties,
12 Permanent Injunction, and Other Relief in the Central District of California. *United States v. Musical.ly,*
13 *et.al*, No. 2:19-cv-01439-ODW-RAO (C.D. Cal. March 27, 2019) (Dkt. No. 10). The order imposed a
14 then record \$5.7 million civil penalty for violations of the COPPA Rule, 16 C.F.R. pt. 312, and Section
15 5 of the FTC Act, 15 U.S.C. § 45; required Defendants to destroy personal information of users under
16 the age of 13; remove accounts of users whose age could not be identified; enjoined Defendants from
17 violating the COPPA Rule; and required Defendants to retain certain records related to compliance with
18 the COPPA Rule and the 2019 Permanent Injunction.

19 7. Musical.ly's quick resolution of the Complaint as well as its name change might have
20 indicated an intent to reform its business practices with respect to the manner in which it handled the
21 personal information of children. Unfortunately, that has not been the case.

22 8. When the United States brought its Complaint against Musical.ly in 2019, it alleged that
23 the app had 65 million registered accounts in the United States. As of 2024, there are more than 170
24 million TikTok users in the United States. Clearly, TikTok continues to grow.

1 9. More specifically, it continues to grow its child audience. In July 2020, TikTok estimated
2 that one-third of its 49 million daily users is 14 or younger.²

3 10. Though TikTok purports to require users creating accounts to report their birthdates, it
4 has consistently and knowingly allowed children to bypass or evade the “age gate” and has continued to
5 impermissibly collect, use, and share data from children who self-identify as being below the age of 13.

6 11. As a result of its continued violations of COPPA and its failure to abide by the terms of
7 the March 27, 2019 Permanent Injunction, on August 2, 2024 the Department of Justice filed a
8 Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief (the “DOJ Complaint”)
9 against TikTok, complaining of TikTok’s continued wrongful collection and misuse of minors’ Personal
10 Information without parental consent in violation of COPPA and its obligations under the 2019
11 Permanent Injunction.

12 12. The DOJ Complaint alleges that throughout the Class Period, Defendants have: (1)
13 knowingly created accounts for children and collected data from those children without first notifying
14 their parents and obtaining verifiable parental consent; (2) failed to honor parents’ requests to delete
15 their children’s accounts and information; and (3) failed to delete the accounts and information of users
16 they know are children. Moreover, the DOJ alleges that its ability to assess the precise magnitude of
17 Defendants’ violations has been stymied by Defendants’ failure to keep records demonstrating its
18 COPPA compliance, as required by the terms of the 2019 Permanent Injunction.

19 13. The Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. § 501, *et seq.*,
20 protects children under 13 years old from having their personal information (“Personal Information”)
21 collected by operators of websites or online services directed to children, or operators with actual
22 knowledge that they are collecting Personal Information online from children under 13, unless their
23 parent has first given verifiable consent. Each time Defendants have collected a child’s personal
24 information without parental notice or verifiable consent or have failed to delete that information at the
25

26 _____
27
28 ² Raymond Zhong & Sheera Frenkel, A Third of TikTok’s U.S. Users May Be 14 or Under, Raising
Safety Questions, N.Y. TIMES (August 14, 2020),

1 request of the child’s parents or upon learning it was collected from a child whose parents were not
2 notified or did not provide verifiable consent, Defendants violated COPPA.

3 14. COPPA violations “shall be treated as a violation of a rule defining an unfair ... act or
4 practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (the “FTC Act”),
5 15 U.S.C. § 57a(a)(1)(B).” In other words, a violation of COPPA constitutes an unfair trade practice
6 under Section 5 of the FTC Act. 15 U.S.C. § 45(a).

7 15. A majority of states, including California, Connecticut, and Florida have enacted laws
8 prohibiting unfair and/or unlawful business practices that are modeled after the FTC Act. These “Little
9 FTC Acts” take interpretive guidance from the FTC Act. Defendants, by their unlawful collection and
10 use of the Personal Information of children under the age of 13 without parental notice or consent have
11 violated these Little FTC Acts.

12 16. Additionally, the conduct of TikTok constitutes unwarranted invasions of privacy in
13 violation of the substantial protections California and Connecticut provide to their citizens. These states
14 recognize the common law right to be free from intrusion upon seclusion, as formulated by § 652B of
15 the Restatement (Second) of Torts, which prohibits intentional intrusion upon the solitude or seclusion
16 of another or his or her private affairs or concerns. In addition, the California Constitution provides
17 California citizens and residents an enumerated right to privacy.

18 17. Defendants’ conduct a) violates the “Little FTC Acts” of California, Connecticut and
19 Florida; (b) the common law right to be free from intrusion upon seclusion in California, and
20 Connecticut; (c); has resulted in Defendants’ unjust enrichment at the expense of minor children in
21 California, Connecticut, and Florida; and (d) violates the right to privacy enumerated in the California
22 Constitution.

23 18. Accordingly, Plaintiffs, through their parents and guardians, bring this action for the
24 relief asserted herein, on behalf of themselves and the Classes of similarly-situated minors whose
25 privacy rights have, like Plaintiffs, been violated by Defendants, for damages, restitution, unjust
26 enrichment, and appropriate injunctive and/or equitable relief to address Defendants’ unlawful practices.

JURISDICTION AND VENUE

19. This Court has general personal jurisdiction over Defendants TikTok, Inc., TikTok Data Security, Inc., and Bytedance, Inc. because their principal places of business are in California. Additionally, all Defendants are subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiffs' claims occurred in this State.

20. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C §1332(d), because the amount in controversy for the Classes exceeds \$5,000,000 exclusive of interest and costs, there are more than 100 potential class members, defined below, and minimal diversity exists because the majority of potential class members are citizens of a state different than Defendants.

21. This Court also has jurisdiction pursuant to 28 U.S.C §1332(d), because the amount in controversy exceeds \$75,000 and is between citizens of different states.

22. Venue is proper in this District pursuant to 28 U.S.C. §1391(b), because a substantial portion of the conduct described in this Complaint was carried out in this District. Furthermore, Defendants TikTok, Inc., and TikTok Data Security, Inc. are headquartered in this District and subject to personal jurisdiction in this District.

PARTIES

I. Plaintiffs

23. Plaintiff A.A. is a natural person and is a resident and citizen of the State of California. A.A. was under the age of 13 during the Class Period. A.A.'s parent and legal guardian is Marcelo Muto, who is also a resident and citizen of the State of California. During the Class Period Plaintiff A.A. had a TikTok account, and regularly viewed content on the platform.

24. Plaintiff A.B. is a natural person and is a resident and citizen of the State of Connecticut. A.B. was under the age of 13 during the Class Period. A.B.'s parent and legal guardian is Heather Bressette, who is also a resident and citizen of the State of Connecticut. During the Class Period, Plaintiff A.B. had a TikTok account and regularly viewed content on the platform

25. Plaintiff A.C. is a natural person and is a resident and citizen of the State of Florida. A.C. was under the age of 13 during the Class Period. A.C.'s parent and legal guardian is Darryl Maulsby, who is also a resident and citizen of the State of Florida. During the Class Period, Plaintiff A.C. had a

1 TikTok account and regularly viewed content on the platform.

2 **II. Defendants**

3 26. Defendant TikTok Inc. is a California corporation with its principal place of business at
4 5800 Bristol Parkway, Suite 100, Culver City, California 90230. TikTok Inc. transacts or has transacted
5 business in this District and throughout the United States.

6 27. Defendant TikTok U.S. Data Security Inc. is a Delaware corporation with its principal
7 place of business shared with TikTok Inc. TikTok U.S. Data Security Inc. transacts or has transacted
8 business in this District and throughout the United States.

9 28. Defendant ByteDance Ltd. is a Cayman Islands company. It has had offices in the United
10 States and in other countries. ByteDance Ltd. transacts or has transacted business in this District and
11 throughout the United States.

12 29. Defendant ByteDance Inc. is a Delaware corporation with its principal place of business
13 at 250 Bryant Street, Mountain View, California, 94041. ByteDance Inc. transacts or has transacted
14 business in this District and throughout the United States.

15 30. Defendant TikTok Pte. Ltd. is a Singapore company with its principal place of business
16 at 8 Marina View Level 43 Asia Square Tower 1, Singapore 018960. TikTok Pte. Ltd. transacts or has
17 transacted business in this District and throughout the United States.

18 31. Defendant TikTok Ltd. is a Cayman Islands company with its principal place of business
19 in Singapore or Beijing, China. TikTok Ltd. transacts or has transacted business in this District and
20 throughout the United States.

21 **SUBSTANTIVE ALLEGATIONS**

22 **FACTUAL BACKGROUND**

23 **I. TikTok Collects and Exploits the Personal Information of Children**

24 **A. The TikTok Platform.**

25 32. TikTok operates a video-based social media platform that consumers may access via the
26 Internet or through a downloadable software application or “app.” In November 2017, ByteDance Ltd.
27 purchased Musical.ly and, in 2018 it merged it into TikTok.

1 33. The TikTok platform allows users to create, upload, and share shortform videos. The
2 TikTok app is free to download. It generates revenue for Defendants through advertising and
3 eCommerce, including through the TikTok for Business platform, as well as in-app purchases of TikTok
4 “coin” through the TikTok Shop.

5 34. TikTok features a “For You” feed in which an algorithm subject to Defendants’ control
6 selects videos for each user based on its determination of their interests, pushes those videos to the user,
7 and plays them.

8 35. TikTok’s algorithms are trained on data collected from users via the TikTok platform and
9 from third-party sources. Such data include videos viewed, “liked,” or shared, accounts followed,
10 comments, content created, video captions, sounds, and hashtags, as well as device and account settings
11 such as language preference, country setting, and device type.

12 36. TikTok was, at all times throughout the Class Period, aware that minor children accessed
13 and engaged with its platform and actively sought to increase viewing and engagement by children
14 through content directed toward those children, while publicly representing that such minors were not
15 permitted to access TikTok’s adult version and were protected by TikTok Kid’s version.

16 **B. Defendants knowingly created accounts for children and collected children’s data**
17 **without parental notice or consent.**

18 37. Since at least March 2019, Defendants have required that users input a birthdate when
19 creating a TikTok account. This is also known as an age-gate.

20 38. Children who self-identify as under the age of 13 in the United States are offered what
21 Defendants refer to as TikTok for Younger Users or “Kids Mode” (hereinafter “Kids Mode”).

22 39. In Kids Mode, a user can view videos, but cannot upload videos, post information
23 publicly, or message other users.

24 40. Parents are neither notified nor asked to consent to the creation of an account in Kids
25 Mode.

26 41. If a user indicates that he or she is over the age of 13, that user is permitted to create an
27 regular account on TikTok.

1 42. Although age-gates are not fool-proof, in response to the DOJ’s 2019 action TikTok
2 implemented a particularly flimsy age-gate that was designed to permit children to continue creating
3 regular TikTok accounts. For instance, the age-gate TikTok implemented allowed children to make
4 multiple attempts at creating an account. Until at least late 2020, a child who input an age below 13
5 could restart the account creation process to put in a different age. Thus, even though Defendants had
6 actual knowledge of a child-user’s age based on the prior attempt to create an account, Defendants
7 permitted children to restart the account process and create regular accounts.

8 43. Another way children could avoid Defendants’ woefully deficient age-gate was to use
9 login credentials from third-party online services such as Instagram and Google. Defendants internally
10 identified these TikTok accounts as “age unknown.” This practice persisted until at least May 2022 –
11 more than three years after TikTok entered into a Permanent Injunction designed to prevent its collection
12 and use of the Personal Information of children.

13 44. These policies and practices led to the creation of millions of accounts for which
14 Defendants did not know the age of the user.

15 45. TikTok’s porous age-gate permitted it to continue collecting the Personal Information of
16 children without parental consent, including first and last name, age, email address, phone number,
17 persistent identifiers for the device(s) used to access TikTok, social media account information, and a
18 profile image, as well as photographs, videos, and audio files containing the user’s image and voice and
19 the metadata associated with such media (such as when, where, and by whom the content was created).

20 46. Over time Defendants collected additional information from these child-users, including
21 usage information, device information, location data, image and audio information, metadata, and data
22 from cookies and similar technologies that track user across different websites and platforms.

23 47. Defendants’ practice of allowing children to sign up for a TikTok account using third-
24 party credentials allowed children to create a TikTok account, gaining access to adult content and
25 features of the general TikTok platform without providing age information. Without parental notice or
26 consent, Defendants then collected and maintained vast amounts of personal information from the
27 children who created and used these TikTok accounts.

1 48. Defendants did not start requiring all users to go through a TikTok age gate until at least
2 2022, closing what employees internally described in early 2021 as an age gate “loophole.”

3 **C. Defendants collected personal information from “Kids Mode” accounts.**

4 49. In Kids Mode, Defendants collect and maintain a username, password, and birthday (day,
5 month, and year). They have also collected several types of persistent identifiers from Kids Mode users
6 without notifying parents or obtaining their consent, including IP address and unique device identifiers.

7 50. The COPPA Rule permits operators to collect a persistent identifier from children under
8 certain circumstances without first obtaining verifiable parental consent, but only if no other personal
9 information is collected and the identifier is used for the sole purpose of providing support for the online
10 service’s internal operations. See 16 C.F.R. § 312.4(c)(7). Defendants’ collection and use of persistent
11 identifiers from Kids Mode users did not comply with this provision and went well beyond what was
12 necessary to operate the TikTok platform. During the Class Period, Defendants additionally collected
13 dozens of other types of information concerning child users with Kids Mode accounts—including app
14 activity data, device information, mobile carrier information, and app information—which they combine
15 with persistent identifiers and used to amass profiles on children.

16 51. Defendants shared information they collected from children in Kids Mode, including
17 persistent identifiers, with third parties without parental consent.

18 52. For example, Defendants shared this information with Facebook and AppsFlyer, a
19 marketing analytics firm, in part to encourage existing Kids Mode users whose use had declined or
20 ceased to use Kids Mode more frequently. Defendants called this process “retargeting less active users.”
21 This practice used children’s personal information for reasons beyond support for the internal operations
22 of Kids Mode and thus was not permitted by the COPPA Rule.

23 53. Separately, users in Kids Mode can send feedback to TikTok using an in-app “Report a
24 Problem” function. When doing so, Defendants require the child to enter the child’s email address.

25 54. Between February 2019 and July 2022, for example, Defendants collected over 300,000
26 problem reports from users in Kids Mode that included children’s email addresses.

27 55. Defendants did not delete these children’s email addresses after processing the reports,
28 and thus retained these email addresses longer than reasonably necessary to fulfill the purpose for which

1 the information was collected, in violation of the Rule. See 16 C.F.R. § 312.10. Defendants did not
2 notify parents of this ongoing practice.

3 **D. Defendants ignored parent requests to delete child users' data.**

4 56. Defendants have allowed millions of children to create TikTok accounts outside of Kids
5 Mode.

6 57. Many children create and maintain accounts without their parents' knowledge.
7 Frequently, however, a parent becomes aware that their child has an account and seeks to have the
8 account and its associated data deleted.

9 58. Despite the fact that regulation and the 2019 Permanent Injunction require Defendants to
10 delete personal information collected from children at their parents' request, in many instances
11 Defendants have obstructed parents' ability to make such requests and have failed to comply with these
12 requests.

13 59. First, Defendants failed to create a simple process for parents to submit a deletion request.
14 For example, the word "delete" does not appear in many of Defendants' online parental guidance
15 materials, such as TikTok's "Guardian's Guide," the "Privacy and Security on TikTok" page, TikTok's
16 "New User Guide," and other materials on tiktok.com such as the "Parental Controls Guide" and "The
17 Parent's Guide to TikTok."

18 60. Second, TikTok required parents to navigate a byzantine process to request deletion of
19 their child's account and information. For example, as recently as 2023, a parent visiting tiktok.com to
20 request deletion of their child's TikTok account and information had to scroll through multiple webpages
21 to find and click on a series of links and menu options that gave no clear indication they apply to such a
22 request. Parents then had to explain in a text box that they are a parent who wanted their child's account
23 and data to be deleted.

24 61. At times, Defendants also directed parents to send their requests to delete their children's
25 accounts and personal information to an email address, then simply failed to respond in a timely manner
26 to these requests, or simply failed to respond to them at all.

27 62. Even if a parent succeeded in submitting a request to delete their child's account and
28 information, Defendants often did not honor that request- instead deferring to self-serving policies

1 intended to prevent deletion of information. In response to each request, Defendants' staff would review
2 the account for "objective indicators" that the account holder was under 13, or "underage," based on the
3 user's handle, biography or "bio." Under Defendants' policy, an account would be identified as an
4 underage account and deleted only if the reviewed elements contained an explicit admission that the
5 user was under 13—for example, "I am in first grade" or "I am 9 years old"—to determine whether a
6 child was younger than 13.

7 63. If these policies were not triggered by Defendants' self-serving review, they would often
8 require parents to re-submit the same information, or additional forms under penalty of perjury. If this
9 secondary form was not completed, Defendants would not delete the minor's data.

10 64. Defendants were aware this was occurring. For example, in a 2018 exchange, a high-
11 level employee of Defendants explicitly acknowledged that Defendants had "actual knowledge" of
12 children on TikTok upon receiving the first parental request, and yet did not delete children's accounts
13 upon receiving the request. In the exchange, the former CEO of TikTok Inc. communicated about
14 underage users on TikTok with the executive responsible for child safety issues in the United States.
15 The employee in charge of child safety issues questioned why parents had to fill out a second form after
16 they already provided the necessary information, noting: "Why we reply with this template everytime
17 [sic] when we already have all the info that's needed? [I]n this case, we already have the username, the
18 name of the reporter, and the age, yet we still reply with the template." He added that if the person
19 reporting the account "doesn't reply then we have actual knowledge of underage user and took no
20 action!"

21 65. Despite this awareness that they were failing to respect parents' deletion requests,
22 Defendants continued using this flawed process through 2023.

23 66. In addition to using what they knew to be a flawed process to address parents' deletion
24 requests, Defendants in many cases did not respond to parents' requests at all. As of late December
25 2020, Defendants had a backlog of thousands of emails dating back months requesting that TikTok
26 delete individual children's accounts

27 67. Defendants' inadequate policies and inaction led to numerous children continuing to
28 maintain TikTok accounts even though their parents had asked Defendants to delete those accounts. In

1 a sample conducted by the Department of Justice of approximately 1,700 children’s TikTok accounts
2 about which Defendants received complaints and deletion requests between March 21, 2019, and
3 December 14, 2020, approximately 500 (30%) remained active as of November 1, 2021. Several
4 hundred of these accounts are likely still active and represent only a small fraction of the thousands of
5 deletion requests Defendants received and failed to act on.

6 68. Compounding these problems, even when Defendants did delete a child’s account and
7 personal information at their parent’s request, at least until recently, Defendants did nothing to prevent
8 the same child from re-creating their account with the same device, persistent identifiers, and email
9 address or phone number as before. This means that a child whose account has been removed could
10 simply create a new account.

11 **E. Defendants did not delete children’s accounts identified by their own systems.**

12 69. Defendants purport to use technology, user reports, and human moderation to identify
13 children’s TikTok accounts so that those accounts and the information collected from them can be
14 deleted. But Defendants know their processes and policies are deficient, and they fail to delete accounts
15 and information that even their own employees and systems identify as belonging to children.

16 70. Since approximately 2020, Defendants have used “keyword matching” purportedly to
17 identify children’s accounts for deletion. Defendants’ keyword matching process searches users’ profiles
18 for terms deemed likely to correspond to child accounts—for example, “4th grade” and “9 years old”—
19 and submits accounts that include those terms for review and potential removal. Defendants’ keyword
20 matching practices have proven woefully deficient.

21 71. Defendants’ human content moderators review accounts flagged as potentially belonging
22 to children by the keyword matching process or by other methods. Similar to Defendants’ restrictive
23 approach to parental deletion requests, the content moderators who review accounts may delete them as
24 belonging to children only if rigid criteria are satisfied.

25 72. Earlier versions of the policy were even more restrictive. For example, to mark and
26 delete an account as underage, the policy between the spring of 2020 and early 2021 required an explicit
27 admission of age, regardless of what videos the account had posted.
28

1 73. Additionally, Defendants' content moderators are not told why an account was flagged
2 as possibly underage. If the policy's rigid criteria are not met, content moderators have no discretion
3 to designate an account as underage; they must allow any such account to remain on the platform even
4 if they know the account holder is in fact a child.

5 74. Defendants have also failed to allow content moderators sufficient time to conduct even
6 the limited review they permit. TikTok often has tens of millions of monthly active users in the United
7 States. Meanwhile, TikTok Inc. 's content moderation team included fewer than two dozen full-time
8 human moderators responsible for identifying and removing material that violated all of its content-
9 related policies, including identifying and deleting accounts of unauthorized users under age 13. At
10 some points, TikTok's human moderators spend an average of less than 10 seconds on each review.

11 75. The deficiency of Defendants' policies is shown by the fact that regular TikTok accounts
12 belonging to children can be easily found by searching for the same basic terms and variations used by
13 Defendants' keyword matching algorithm. Some of these accounts have existed for long periods—able
14 to garner hundreds of followers and hundreds or even thousands of “likes,” a sign of approval by other
15 TikTok users.

16 76. By adhering to these deficient policies, Defendants actively avoid deleting the accounts
17 of users they know to be children. Instead, Defendants continue collecting these children's Personal
18 Information, showing them videos not intended for children, serving them ads and generating revenue
19 from such ads, and allowing adults to directly communicate with them through TikTok.

20 **F. TikTok had actual knowledge that it was collecting, storing and using the personal**
21 **information of children under the age of 13.**

22 77. Many accounts that belong to children come to Defendants' attention when one user
23 reports another user's video as violating one of Defendants' policies. Those videos are then added to
24 “video queues” and reviewed by human content moderators who review the videos to determine whether
25 they comply with Defendants' policies. If those content moderators encounter a video that depicts a
26 child under 13, they can apply labels to designate suspected child users, such as “Content Depicting
27 Under the Age of Admission” or “Suspected Underaged User.” These moderators can remove a specific
28 video from TikTok, but they lack authority to delete or remove the account even if it is clearly the

1 account of a child. Instead, by applying the labels, they refer the video to the separate content moderation
2 team that assesses whether accounts belong to underage users (the “underage queue”).

3 78. During the Class Period, however, the process did not work. Accordingly, when
4 Defendants’ moderators tagged specific videos as depicting a child under 13, the associated accounts
5 were not actually referred to the team authorized to delete the associated account. Instead, those accounts
6 remained live, and Defendants continued to collect and retain those children’s personal information and
7 to show them videos and messages from adult TikTok users. Due to Defendants’ recordkeeping
8 deficiencies, detailed below, they cannot identify the number of accounts affected by this issue. The
9 limited records Defendants do have, however, make clear that millions of accounts were involved.

10 79. Defendants conduct quality assurance reviews of the content moderation processes
11 described above. The quality assurance reviews require content moderators to re-review a subset of
12 previously reviewed accounts or videos. This process aims to identify instances in which TikTok content
13 moderators incorrectly applied company policies to those accounts or videos.

14 80. Until at least September 2022, however, when Defendants’ quality assurance analysts
15 identified a specific account that a moderator incorrectly failed to flag for deletion as belonging to a
16 child, Defendants did not then go back and delete the account. Instead, the account remained live.
17 Accordingly, Defendants failed to delete numerous children’s accounts that their own quality assurance
18 team specifically identified as belonging to children.

19 81. Even where accounts satisfied Defendants’ rigid criteria, were identified as belonging to
20 children, and were marked for deletion, Defendants failed to delete many of the accounts.

21 82. Internal communications reveal that Defendants’ employees were aware of this issue. In
22 a September 2021 online chat, for example, employees discussed the fact that accounts were being
23 marked as banned for being underage but were not being deleted and suggested this had been occurring
24 since mid-July 2020. One employee noted that she was seeing this “a lot” and “I run across usually like
25 3-4 accounts [like that] a day,” while another noted “[t]hat shouldn’t be happening at all or we can get
26 in trouble ... because of COPPA.” TikTok knew that many of its account holders were under 13 years
27 of age.
28

1 83. Although Defendants were unquestionably aware of the problem and were under a Court
2 Order to keep records of their COPPA compliance, they failed to do so.

3 84. In addition to Defendants' unlawful collection and use of the Personal Information of
4 children under 13, Defendants retain children's Personal Information long after they identify an account
5 as belonging to a child and determine they should delete information related to the account. For example,
6 Defendants retain app activity log data related to children for 18 months.

7 85. Defendants have retained children's Personal Information in numerous database
8 locations long after purportedly deleting their accounts. Defendants have not documented what
9 information collected from users is saved in what locations or why, and they have been unable to explain
10 how or why the information was in those locations, or why it was not deleted and failed to delete
11 information children posted to TikTok that was later incorporated into other users' videos, even when
12 Defendants possessed identifiers linking the information to an account that they deleted because it
13 belonged to a child.

14 86. Similarly, Defendants retained profile photographs of users that Defendants knew to be
15 children. For example, TikTok allows users to include in their videos another user's comment, which is
16 displayed alongside the commenter's photograph and username. When Defendants did "delete" the
17 account of a child, that child's comments remained in other users' posts, along with their photograph
18 and username. These images had unique identifiers that tied each child's photograph, username, and
19 comment to an account that Defendants knew had been deleted because it belonged to a child.

20 87. Defendants' internal analyses show that millions of TikTok's U.S. users are children
21 under the age of 13. For example, the number of U.S. TikTok users that Defendants classified as age 14
22 or younger in 2020 was millions higher than the U.S. Census Bureau's estimate of the total number of
23 13- and 14-year olds in the United States, suggesting that many of those users were children younger
24 than 13.

25 88. Defendants and their employees have long known that children misrepresent their ages
26 to pass through TikTok's age gate. For example, in 2020, a TikTok moderator recognized that
27 Defendants maintain accounts of children despite the "fact that we know the user is U13," i.e., under
28 age 13, so long as the child's profile does not admit that fact explicitly. Another employee admitted that

1 TikTok moderators were required to ignore any “external information” indicating that a user under
2 review is a child.

3 89. In another example, in a July 2020 chat, one of Defendants’ employees circulated the
4 profiles of numerous underage users he had identified “literally through one minute of scanning,” noting
5 “[t]his is incredibly concerning and needs to be addressed immediately.”

6 90. Defendants have other methods available to them to identify and remove children’s
7 accounts from the TikTok platform -- but purposely do not use them. For example, TikTok has its own
8 age-determining technology— “grade level.” The grade level algorithm is based on users’ online
9 behavior and other metrics for purposes such as advertising. Unlike TikTok’s age gate, this method is
10 based on observable behaviors and not solely users’ self-reported age. However, despite their knowledge
11 of the violations of law alleged herein, Defendants have not used it to attempt to identify children on the
12 platform for the purpose of removing accounts that violate COPPA.

13 91. In fact, Defendants have programmed grade level to avoid gaining knowledge that users
14 were under 13. In 2020, Defendants’ lowest age group band was for ages under 15, meaning that it
15 would not identify users as under 13 specifically. Defendants later revised this age cutoff so that the
16 lowest age segment was under 16.

17 92. TikTok had actual knowledge that children under 13 were using TikTok yet did not obtain
18 verifiable parental consent before collecting the Personal Information of those children in violation of
19 COPPA, the FTC Act, and the consumer protection laws of many states. These acts also constituted an
20 intrusion upon the seclusion of children under 13 as well as a violation of their reasonable expectation of
21 privacy.

22 **G. TikTok made false claims to the FTC about its COPPA compliance.**

23 93. One June 12, 2020 TikTok Inc. stated to the FTC that “[o]n May 11, 2019...[it] took
24 offline all US accounts that did not go through [its recently imposed] age gate. These accounts...were
25 not accessible to the Company. TikTok did not use or disclose the information for any purpose.”
26 TikTok Inc. also stated that it “completed on May 24, 2020” the deletion of children’s data as required
27 by the 2019 Permanent Injunction. V Pappas, as “GM of TikTok,” certified on TikTok Inc.’s behalf
28 under penalty of perjury that the prior statement was true and correct.

94. According to the August 2, 2024 DOJ Complaint, after follow-up inquiry by the FTC, TikTok Inc. acknowledged that its June 12, 2020 claims had been false. In fact, TikTok Inc. retained and used data that it previously represented it “did not use,” and was “not accessible” to it, and was “delet[ed].” That data included Personal Information and other data of child, teen, and adult users, including IP addresses, device IDs, device models and advertising IDs.

II. Defendants Knowingly Collected and Exploited the Personal Information of Children Without Parental Consent in Violation of COPPA, State Unfair Trade Practices Statutes, and Common Law and Constitutional Prohibitions Against the Invasion of Privacy.

A. The Children’s Online Privacy Protection Act of 1998.

95. Congress passed COPPA, codified at 15 U.S.C. § 6501, *et seq.*, in 1998 in response to concerns that children’s online activities were being tracked by operators of websites and online services. COPPA is intended to “maintain the security of personally identifiable information of children collected online” and to “protect children’s privacy by limiting the collection of personal information from children without parental consent.”³ The standards in COPPA have given rise to, and correlate with, accepted norms throughout society for defining the expectations of privacy for minor children.

96. COPPA applies to any operator of a commercial website or online service directed to children under 13 years of age that collects, uses, and/or discloses Personal Information from children. The FTC considers parties with actual knowledge that they are collecting Personal Information from users of a child-directed site or service as “operators” under COPPA.

97. COPPA “prohibits unfair ... acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.” 16 C.F.R. § 312.1.

98. COPPA provides, in pertinent part, that:

It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information

³ 144 CONG. REC. S12787.

1 from a child, to collect personal information from a child in a manner that violates
2 the regulations prescribed [by the Federal Trade Commission]. 15 U.S.C. § 6502(a).

3 99. COPPA thus prohibits, *inter alia*, the collection of persistent identifiers for behavioral
4 advertising absent notice and verifiable parental consent. 16 C.F.R. §§ 312.5(c)(7), 312.2.

5 100. COPPA specifically requires an “operator” covered by COPPA to give notice to parents
6 and obtain their verifiable consent before collecting children’s Personal Information online. 16 C.F.R.
7 §§ 312.4 and 312.5. This includes but is not limited to:

- 8 a. Posting a privacy policy on its website or online service providing clear,
9 understandable, and complete notice of its information practices, including what
10 information the website operator collects from children online, how it uses such
11 information, its disclosure practices for such information, and other specific
12 disclosures set forth by COPPA;
- 13 b. Providing clear, understandable, and complete notice of its information practices,
14 including specific disclosures directly to parents; and
- 15 c. Obtaining verifiable parental consent prior to collecting, using, and/or disclosing
16 Personal Information from children.

17 101. The FTC has interpreted “operators of website or online services directed to children”
18 and “operators with actual knowledge that they are collecting personal information online from children
19 under 13” “subject to strict liability for COPPA violations.”⁴

20 102. Websites or online services that collect Personal Information from users of other child-
21 directed websites or online services are deemed as “child-directed” if the website or online service “has
22 actual knowledge that it is collecting personal information directly from users of another Web site or
23 online service directed to children.” 16 C.F.R. § 312.2.

24
25
26 ⁴ Statement of Joseph J. Simons & Christine S. Wilson, *Regarding FTC and People of the State of New*
27 *York v. Google LLC and YouTube, LLC*, FEDERAL TRADE COMMISSION, [https://www.ftc.gov/](https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf)
28 [system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf](https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf)
(accessed Oct. 21, 2019).

1 103. In order to determine whether a website or online service is “directed to children” the
2 FTC will:

3 [C]onsider [the website’s or online service’s] subject matter, visual content, use of
4 animated characters or child-oriented activities and incentives, music or other audio
5 content, age of models, presence of child celebrities or celebrities who appeal to
6 children, language or other characteristics of the Web site or online service, as well
7 as whether advertising promoting or appearing on the Web site or online service is
8 directed to children.

9 16 CFR § 312.2

10 104. In 2013, COPPA was enhanced (the “2013 COPPA Enhancement”) to provide further
11 protection for children against online tracking and to “giv[e] parents greater control over the online
12 collection of their children’s personal information.” The 2013 enhancement widened the definition of
13 children’s “Personal Information” to include “persistent identifiers” such as cookies that track a child’s
14 activity online, geolocation information, photos, videos, and audio recordings.

15 105. The 2013 COPPA Enhancement was the culmination of two years of rulemaking by the
16 FTC and reflected society’s growing recognition of the surreptitious surveillance tactics used by
17 advertising companies to track children online and advertise to them while using the internet.

18 106. By expressly including persistent identifiers and geolocation data in COPPA’s definition
19 of Personal Information, the FTC intended to deter advertising companies and internet operators such
20 as TikTok from exploiting young children via tracking, profiling, and advertising online.

21 107. Pursuant to Section 1303(c) of COPPA, 15 U.S.C. § 6502(c), and Section 18(d)(3) of the
22 FTC Act, 15 U.S.C. § 57a(d)(3), a violation of COPPA constitutes an unfair ... act or practice in or
23 affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

24 108. While COPPA does not itself provide a private right of action for individuals to seek
25 redress for harms arising from COPPA violations, and contains a limited preemption clause barring the
26 imposition of liability by states and local governments “inconsistent” with COPPA (15 U.S.C. §
27 6502(d)), the United States Court of Appeals for the Ninth Circuit has held that “COPPA’s preemption
28 clause does not bar state-law causes of action that are parallel to, or proscribe the same conduct forbidden
by, COPPA.” *Jones v. Google LLC*, 73 F.4th 636 (9th Cir. 2023).

1 109. Therefore, individuals harmed by conduct which violates COPPA such as the conduct
2 described herein may seek redress for harms via state law causes of action.

3 **B. Defendants’ tracking, profiling, targeting and exploitation of children without**
4 **parental consent constitutes unfair and unlawful conduct.**

5 110. State legislatures across the country have enacted consumer protection statutes
6 proscribing the same unfair and unlawful business conduct proscribed by the FTC Act and rules
7 promulgated thereunder. These “Little FTC Acts” were often enacted for the specific purpose of
8 supplementing the FTC’s mission of protecting consumers from unfair and/or unlawful acts or practices
9 by providing state citizens with a private right of action to seek redress for harm arising out of acts those
10 acts which are also prohibited by the FTC Act, which lacks a private right of action.

11 111. Thus, the conduct which the FTC determined violated COPPA jointly carried out by
12 Defendants as described above, not only constitutes “unfair” and therefore unlawful acts that violate
13 COPPA and the FTC Act, but also constitutes “unfair” and therefore unlawful acts pursuant to the Little
14 FTC Acts.

15 112. Specifically, the acts carried out by Defendants described above constitute “unfair” acts
16 under the Little FTC Acts pursuant to which Plaintiffs bring claims because they caused substantial injury
17 to Plaintiffs and those similarly situated by intrusively and invasively collecting and using their Personal
18 Information without notice or parental consent in violation of COPPA, the FTC Act, and societal norms.
19 These injuries could not be reasonably avoided by the vulnerable children under 13 years of age that
20 TikTok targeted. Nor were the injuries to Plaintiffs and similarly situated children in the United States
21 caused by TikTok Defendants outweighed by countervailing benefits to consumers.

22 **C. Defendants’ tracking, profiling, targeting and exploitation of children without**
23 **parental consent violated Plaintiffs’ and Class members’ reasonable expectations of**
24 **privacy and is highly offensive.**

25 113. TikTok’s conduct in violating the privacy rights and reasonable expectations of privacy
26 of Plaintiffs and Class members by implementing a flawed-by-design age-gating system is particularly
27 egregious because TikTok agreed to cease this behavior in the 2019 Permanent Injunction. Defendants’
28 actions have violated norms and laws designed to protect children – a group that society has long
recognized is vulnerable to exploitation and manipulation.

1 114. Parents' interest in the care, custody, and control of their children is one of the most
 2 fundamental liberty interests recognized by society. It has long been recognized that parents should
 3 maintain control over who interacts with their children and how.

4 115. Because children are more susceptible to exploitation than adults, society has recognized
 5 the importance of providing added legal protections for children, often in the form of parental consent
 6 requirements.

7 116. In fact, as discussed above, the FTC's enhancements of COPPA in 2013 reflect a specific
 8 concern with mobile app tracking and tracking internet users via persistent identifiers, and reflect the
 9 offensiveness with which society regards this behavior.

10 117. Children develop the ability to use smartphones and tablets by the age of two.⁵ Almost
 11 every family with a child younger than eight in America has a smartphone (95%) and/or tablet (78%) in
 12 the household.⁶

13 118. Often, children are given their own devices, with one 2015 study finding that by age four,
 14 75% of children had their own tablet, smartphone, or iPod.⁷

15 119. Nearly all parents in the United States (94%) say their children under 13 use online apps,
 16 with top apps used being video streaming (64%), video gaming (58%) and show/movie streaming
 17 (58%).⁸

21 ⁵ Elyse Wanshel, *10 Reason Why You Shouldn't Give a Child a Smartphone or Tablet*, LITTLE THINGS,
 22 <https://www.littlethings.com/reasons-not-to-give-children-technology> (accessed Oct. 21, 2019).

23 ⁶ Victoria Rideout, *The Common Sense Census: Media Use By Kids Age Zero To Eight*, COMMON SENSE
 24 MEDIA (2017) at 3, <https://www.common sense media.org/research/the-common-sense-census-media-use-by-kids-agezero-to-eight-2017> (accessed Oct. 21, 2019).

25 ⁷ *The Dangers of YouTube for Kids*, THE ATLANTIC (Nov. 2018), <https://www.theatlantic.com/magazine/archive/2018/11/raised-by-youtube/570838/> (accessed Oct. 22, 2019) ("[A] team of
 26 pediatricians at Einstein Medical Center, in Philadelphia, found that YouTube was popular among
 27 device-using children under the age of 2. Oh, and 97 percent of the kids in the study had used a mobile
 28 device. By age 4, 75 percent of the children in the study had their own tablet, smartphone, or iPod. And
 that was in 2015.).

⁸ <https://www.pixalate.com/blog/childrens-online-privacy-harris-poll-recap>.

120. Four in five parents (80%) whose children under 13 use online apps say they worry about their children's privacy when using those apps,⁹ with the top concern (69%) being data tracking.¹⁰

121. Nearly 3 in 4 parents whose children under 13 use online apps (73%) say they are concerned about their children's location being tracked by those apps; those residing in urban or rural areas are more likely than those residing in suburban areas to share this sentiment (88% and 87% vs. 73%).¹¹

122. More than three-quarters (77%) of parents are concerned about protecting their family's digital privacy.¹²

123. 73% of parents are concerned about personal data being collected by third parties, without their consent.¹³

124. And parents also recognize the importance of protecting their children's identity (90%), location (88%), health data (87%), age (85%), school records (85%), and browsing history (84%).¹⁴

125. Additionally, a survey conducted by the Center for Digital Democracy ("CDD") and Common Sense Media of more than 2,000 adults found overwhelming support for the basic principles of privacy embedded in the California Constitution, state common law, as well as federal law.¹⁵ The parents who were polled responded as follows when asked whether they agreed or disagreed with the following statements:

⁹ *Id.*

¹⁰ <https://www.cdpinstitute.org/news/childrens-privacy-data-tracking-is-a-big-concern-for-parents-and-trust-levels-in-companies-are-low/>.

¹¹ <https://www.pixalate.com/blog/childrens-online-privacy-harris-poll-recap>.

¹² <https://trustedfuture.org/childrens-digital-privacy-and-safety>.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ Center for Digital Democracy, *Survey on Children and Online Privacy, Summary of Methods and Findings*, <https://www.democraticmedia.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf> (accessed Oct. 21, 2019).

- 1 a. “It is okay for advertisers to track and keep a record of a child’s behavior online if they
2 give the child free content.”
- 3 • 5 percent strongly agree
 - 4 • 3 percent somewhat agree
 - 5 • 15 percent somewhat disagree
 - 6 • **75 percent strongly disagree**
 - 7 • 3 percent do not know or refused to answer
- 8 b. “As long as advertisers don’t know a child’s name and address, it is okay for them to
9 collect and use information about the child’s activity online.”
- 10 • 3 percent strongly agree
 - 11 • 17 percent somewhat agree
 - 12 • 10 percent somewhat disagree
 - 13 • **69 percent strongly disagree**
 - 14 • 1 percent do not know or refused to answer
- 15 c. “It is okay for advertisers to collect information about a child’s location from that child’s
16 mobile phone.”
- 17 • 6 percent strongly agree
 - 18 • 3 percent somewhat agree
 - 19 • 7 percent somewhat disagree
 - 20 • **84 percent strongly disagree**
 - 21 • less than 1 percent do not know or refused to answer
- 22 d. “Before advertisers put tracking software on a child’s computer, advertisers should
23 receive the parent’s permission.”
- 24 • **89 percent strongly agree**
 - 25 • 5 percent somewhat agree
 - 26 • 2 percent somewhat disagree
 - 27 • 4 percent strongly disagree
 - 28 • less than 1 percent do not know or refused to answer

e. “There is a federal law that says that online sites and companies need to ask parents’ permission before they collect Personal Information from children under age 13. Do you think the law is a good idea or a bad idea?”

- **93 percent said it was a good idea**
- 6 percent said it was a bad idea
- 1 percent did not know or refused to answer.

126. The proliferation of internet-connected device usage by children under 13, coupled with the concerns expressed by parents, and Defendants’ past acknowledgment of its failure to adequately protect children and its Court Ordered promise to remediate its practices, renders Defendants’ conduct highly offensive and an egregious breach of social norms.

127. TikTok’s unfair and unlawful collection of Personal Information substantially affects the amount of time minor children, including children under the age of 13, spend on TikTok.

128. By failing to (i) obtain parental consent, (ii) disclose to parents the nature and purpose of their data collection practices (and use of that data), and (iii) take other steps to preclude the capture of children’s Personal Information, and by manipulating and exploiting the habits of minors for their economic gain, Defendants have breached the privacy rights and reasonable expectations of privacy of Plaintiffs’ minor children and the millions of minors in the Classes who have used TikTok’s platform, in contravention of privacy norms that are reflected in consumer surveys, centuries of common law, state and federal statutes, legislative commentaries, industry standards and guidelines, and scholarly literature.

D. Targeting Children in Violation of COPPA and the 2019 Permanent Injunction Commercial Activity into Highly Offensive, Egregious Conduct.

129. Defendants’ abject and intentional failure to abide by the terms of the 2019 Permanent Injunction to ensure its compliance with COPPA has resulted in the continued collection and exploitation of the Personal Information of children for profit and represents a stark departure from long-standing societal and legal traditions that are designed to protect minors from exposure to harmful and addictive activities and/or products. For decades, the United States has recognized the inherent vulnerability of children and has instituted robust regulatory frameworks to shield them from the harms associated with addictive substances and behaviors, such as tobacco, firearms, alcohol, and gambling.

1 130. These protections include age restrictions on the use of addictive or dangerous products
2 such as tobacco, firearms, alcohol, and gambling *and* restrictions on advertising directed towards young
3 children concerning the same. This dual pronged approach of restricting access/use and advertising is
4 rooted in societal consensus that children, by virtue of their developmental stage, require heightened
5 safeguards to ensure their health, well-being, and future potential.¹⁶

6 131. Commercial actors who have ignored these societal values and regulations have been
7 punished severely, reflecting society's view that commercially exploiting children by exposing them to
8 harmful and/or dangerous activities and products is unacceptable. For example, the 1998 Master
9 Settlement Agreement between the attorneys general of 46 states and the American tobacco industry
10 condemned the cigarette companies' targeting of their harmful and addictive products to minors and
11 resulted in a payment of over \$206 billion over 25 years, and barred tobacco companies from using
12 cartoon characters (such as Joe Camel), sponsoring youth-oriented events, and placing ads near schools.

13 132. More recently, in 2022, Juul agreed to pay over \$700 million (\$438.5 million to settle
14 investigations by 34 states and U.S. territories, and \$300 to private plaintiffs) to settle litigation
15 concerning its marketing and sales practices which were alleged to improperly target minors.
16 Investigations had found that Juul's advertising appealed to young people, using influencers and social
17 media to promote its products. The settlement included stringent restrictions on Juul's marketing, sales,
18 and distribution practices to prevent future targeting of youth.

19 133. The egregiousness of Defendants' conduct in knowingly and intentionally instituting an
20 age-gating system that was designed to be by-passed by children under the age of 13, implementing
21 policies and procedures that made it extremely difficult for parents to delete their children's personal
22 information from TikTok, failing to use readily available tools to monitor the presence of underage users,
23

24
25 ¹⁶ See, e.g. *Family Smoking Prevention and Tobacco Control Act*, 21 U.S.C. §§ 387a-387u (restricting
26 manufacture, marketing, and distribution of tobacco products to protect the public health generally and
27 to reduce tobacco use by minors); *Stop Tobacco Access to Kids Enforcement (STAKE) Act*, Cal. Bus. &
28 Prof. Code § 22958 (West 2023) (restricting sale of tobacco products in California to people 21 years of
age or older); *National Minimum Drinking Age Act of 1984*, 23 U.S.C. § 158 (1984) (establishing
minimum age requirement of 21 years old to drink alcohol).

1 and failing to document its COPPA compliance as it was *required* to do by the terms of the 2019
2 Permanent Injunction is manifest.

3 134. Defendants took affirmative steps to avoid the specific obligations they undertook to
4 protect children as part of the resolution of a previous government complaint. Their deliberate and
5 unlawful actions have caused substantial harm to plaintiffs for which they deserve compensation and
6 injunctive relief that will require Defendants to (finally) comply with their obligations under COPPA.

7 **III. Plaintiffs and The Members of The Classes have Suffered Economic Loss and Injury as a**
8 **Result of Defendants' Unfair and Deceptive Conduct.**

9 135. Courts have recognized that internet users have a property interest in their Personal
10 Information and that Personal Information is, thus, an asset with economic value.¹⁷ Through their unfair
11 and deceptive conduct, Defendants misappropriated the Personal Information of Plaintiffs and the
12 members of the Classes, destroyed the principal aspect of the Personal Information that provided its value
13 to Plaintiffs and the members of the Classes, and diminished the value of the Personal Information.

14 136. As a result of Defendants' unfair and deceptive conduct, Plaintiffs and the members
15 of the Classes have, thus, suffered economic loss and injury in one or more of the following respects:

- 16 a. Defendants unlawfully took possession of and commercially exploited the
17 Personal Information of Plaintiffs and the members of the Classes without their
18 permission and without compensation; and
- 19 b. Defendants' unlawful collection and exploitation of the Personal Information of
20 Plaintiffs and the members of the Classes have destroyed the private quality of the
21 Personal Information and have deprived Plaintiffs and the members of the Classes
22 of the ability to determine whether or not to keep their Personal Information
23 private and when or if to sell their Personal Information -- valuable aspects of
24 their rights of ownership that were of paramount importance to Plaintiffs and the

25
26
27 ¹⁷ See *CTC Real Estate Servs. v. Lepe*, 140 Cal. App. 4th 856, 860, 44 Cal.Rptr.3d 823 (2006) ("A
28 person's identifying information is a valuable asset."); accord *Facebook Tracking*, 956 F.3d 589, 600
(9th Cir. 2020) (citing *Lepe* and holding that the plaintiffs had suffered economic injury after Facebook
allegedly took their personal information in a similar process to that alleged here).

members of the Classes in this case – and, thus, diminished the value of the Personal Information.

A. Personal information is an asset that has economic value.

137. The information TikTok collects and uses had and continues to have massive economic value. This value is well understood in the e-commerce industry, and Personal Information is now viewed as a form of currency.

138. Research on the market for Personal Information dates back well before the Class Period,¹⁸ and demonstrates a growing consensus that consumers' sensitive and valuable Personal Information would become the new frontier of financial exploit.

139. Professor Paul M. Schwartz noted in the Harvard Law Review:

Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.¹⁹

140. Likewise, in *The Wall Street Journal*, former fellow at the Open Society Institute (and current principal technologist at the ACLU) Christopher Soghoian noted:

The dirty secret of the Web is that the “free” content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.

¹⁸ “Markets and Privacy” by Kenneth C. Laudon, Communications of the ACM, 1996. https://canvas.harvard.edu/files/4164376/download?download_frd=1.

¹⁹ Paul M. Schwartz, Property, *Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

1 141. Although we now regularly trade our most private information for access to social-
 2 networking sites and free content, the terms of this exchange were never clearly communicated to
 3 consumers.²⁰

4 142. As the thirst has grown for Personal Information,²¹ it has become apparent that the world's
 5 most valuable resource is no longer oil, but instead consumers' data in the form of their Personal
 6 Information.²²

7 143. The cash value of the Personal Information unlawfully collected by TikTok during the
 8 Class Period can be quantified. For example, in a study authored by Tim Morey, researchers studied the
 9 value that 180 internet users placed on keeping personal data secure.²³ Contact information of the sort
 10 that TikTok requires was valued by the study participants at approximately \$4.20 per year. Demographic
 11 information was valued at approximately \$3.00 per year. However, web browsing histories were valued
 12 at a much higher rate: \$52.00 per year. The chart below summarizes the findings:

13
14
15
16
17
18 ²⁰ Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL
 STREET JOURNAL (Nov. 15, 2011).

19 ²¹ *Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value*,
 20 OECD Digital Economy Paper No. 220 at 7 (Apr. 2, 2013), [http://dx.doi.org/10.1787/5k486qtxldmq-](http://dx.doi.org/10.1787/5k486qtxldmq-en)
 21 [en](https://www.oecd.org/sti/inno/newsourcesofgrowthknowledge-basedcapital.htm); *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD, at 319 (Oct. 13,
 22 2013), <https://www.oecd.org/sti/inno/newsourcesofgrowthknowledge-basedcapital.htm>; Pauline
 23 Glickman and Nicolas Glady, *What's the Value of Your Data?* TechCrunch (Oct. 13, 2015)
 24 <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/>; Paul Lewis and Paul Hilder, *Former*
Cambridge Analytica exec says she wants lies to stop, The Guardian (March 23, 2018)
[https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-](https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies)
kaiser-wants-to-stop-lies; Shoshanna Zuboff, *The Age of Surveillance Capitalism* 166 (2019).

25 ²² *The world's most valuable resource is no longer oil, but data*, The Economist (May 6, 2017),
 26 [https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-](https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data)
 longer-oil-but-data.

27 ²³ Tim Morey, *What's Your Personal Data Worth?* DESIGN MIND (Jan. 18, 2011),
 28 [https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039s-your-](https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html)
 personal-data-worth.html.



144. Similarly, the study *Your Browsing Behavior for a Big Mac: Economics of Personal Information Online* by Juan Pablo Carrascal and colleagues employed a detailed methodology to understand how users value their Personal Information in exchange for internet-based services.²⁴ Participants installed a browser plugin that logged their web browsing activities, including the URLs visited and the time of access.²⁵ The plugin also categorized the websites into eight predefined categories: Email, Entertainment, Finance, News, Search, Shopping, Social, and Health and asked participants questions designed to gather information about their perceptions of privacy, their knowledge of how their Personal Information might be monetized, and their valuation of specific pieces of PI as they visited certain websites.²⁶ To calculate the value users placed on their Personal Information, Carrascal and colleagues employed a reverse second-price auction mechanism in which participants bid on the minimum amount of money they would accept to sell specific pieces of their Personal Information in exchange for internet-based services they were using.²⁷

²⁴ Juan Pablo Carrascal et al., *Your Browsing Behavior for a Big Mac: Economics of Personal Information Online*, arXiv preprint arXiv:1112.6098 (2011), <https://arxiv.org/abs/1112.6098>.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

1 145. The results of Carrascal's study were the following Personal Information valuations:

- 2 a. Offline information (age address, economic stats): €25
- 3 b. Browsing History: €7
- 4 c. Interactions on social networks: €12
- 5 d. Search History: €2
- 6 e. Shopping Activity: €5

7 146. What these studies, and others²⁸ show is that individuals place an economic value on their
 8 Personal Information and are willing to engage in economic transactions in which grant access to their
 9 Personal Information in exchange for internet-based services. Defendants' unauthorized collection of
 10 Plaintiffs and Class members Personal Information deprived them of this opportunity.

11 147. On the open market, Personal Information is often mined, compiled, and resold by
 12 data brokers. Further, there is a market for consumers to monetize Personal Information and the
 13 behavioral preferences that Defendants have usurped. Published analyses and studies have placed a value
 14 in excess of \$200 on an individual's Personal Information.²⁹

15 148. A child's Personal Information has equivalent (or potentially greater) value than that of
 16 an adult. It is well-established that children are more susceptible to being influenced by advertisements
 17 and often cannot tell the difference between content and advertisements in child-directed videos. And
 18 Defendants may be able to utilize children's Personal Information to show them behavior-targeted
 19 advertising for the duration of their lives.

20 149. Personal Information also has a value based on consumers' privacy interests. In a recent
 21 study by the Pew Research Center, 93% of Americans said it was "important" for them to be "in control
 22

23
 24 ²⁸ Jacopo Staiano et al., *Money Walks: A Human-Centric Study on the Economics of Personal Mobile*
 25 *Data*, arXiv preprint arXiv:1407.0566 (2014), <https://arxiv.org/abs/1407.0566> (finding that location
 26 information is the most valued type of personal data, with a median value of approximately €25, and
 27 that participants showed significant sensitivity towards monetizing their personal information
 28 collected via mobile phones).

²⁹ *Can you Put a Price on Your Personal Data*, June 28, 2019, NYTimes, <https://www.nytimes.com/2019/06/28/technology/data-price-big-tech.html>.

of who can get information” about them. Seventy-four percent said it was “very important.”³⁰ Eighty-seven percent of Americans said it was “important” for them not to have someone watch or listen to them without their permission.³¹ Sixty-seven percent said it was “very important.”³² And 90% of Americans said it was “important” that they be able to “control[] what information is collected about [them].”³³ Sixty-five percent said it was very important.³⁴

150. Likewise, in a 2011 Harris Poll study, 76% of Americans agreed that “online companies, such as Google or Facebook, control too much of our personal information and know too much about our browsing habits.”³⁵

151. During the Class Period, a number of platforms have appeared that allow consumers to directly monetize their own data and prevent tech companies from targeting them absent their express consent:

- a. Brave’s web browser, for example, will pay users to watch online targeted ads, while blocking out everything else.³⁶

³⁰ <https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/#:~:text=93%25%20of%20adults%20say%20that,it%20is%20%E2%80%9Csomewhat%20important.%E2%80%9D>

³¹ *Id.*

³² *Id.*

³³ *Id.*

³⁴ *Id.*

³⁵ <https://www.prnewswire.com/news-releases/majorities-think-some-online-companies-are-too-powerful-121986453.html>.

³⁶ Get Paid to Watch Ads in the Brave Web Browser, at: <https://lifelacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279#:~:text=Brave%2C%20a%20chromium-based%20web%20browser%20that%20boasts%20an,a%20more%20thoughtful%20way%20than%20we%E2%80%99re%20accustomed%20to> (Lifelacker, April 26, 2019) (“The model is entirely opt-in, meaning that ads will be disable by default. The ads you view will be converted into Brave’s cryptocurrency, Basic Attention Tokens (BAT), paid out to your Brave wallet monthly”).

- b. Loginhood states that it “lets individuals earn rewards for their data and provides website owners with privacy tools for site visitors to control their data sharing,” via a “consent manager” that blocks ads and tracking on browsers as a plugin.³⁷
- c. Andrew Yang’s “Data Dividend Project” aims to help consumers, “[t]ake control of your personal data. If companies are profiting from it, you should get paid for it.”³⁸
- d. Killi is a new data exchange platform that allows consumers to own and earn from their data.³⁹
- e. Similarly, BIGtoken “is a platform to own and earn from your data. You can use the BIGtoken application to manage your digital data and identity and earn rewards when your data is purchased.”⁴⁰
- f. The Nielsen Company, famous for tracking the behavior of television viewers’ habits, has extended its reach to computers and mobile devices through the Nielsen Computer and Mobile Panel. By installing the application on a consumer’s computer, phone, tablet, e-reader, or other mobile device, Nielsen tracks the user’s activity, enters that user into sweepstakes with monetary benefits, and allows the user to earn points worth up to \$50 per month.⁴¹

³⁷ <https://loginhood.io/>. See also, <https://loginhood.io/product/chrome-extension> (“[s]tart earning rewards for sharing data – and block others that have been spying on you. Win-win.”).

³⁸ How Does It Work, at: <https://www.datadividendproject.com/> (“Get Your Data Dividend...We’ll send you \$\$\$ as we negotiate with companies to compensate you for using your personal data.”).

³⁹ <https://killi.io/earn/>.

⁴⁰ https://bigtoken.com/faq#general_0 (“Third-party applications and sites access BIGtoken to learn more about their consumers and earn revenue from data sales made through their platforms. Our BIG promise: all data acquisition is secure and transparent, with consumers made fully aware of how their data is used and who has access to it.”).

⁴¹ Kevin Mercandante, Ten Apps for Selling Your Data for Cash, Best Wallet Hacks (June 10, 2020), <https://wallethacks.com/apps-for-selling-your-data/>.

1 152. Technology companies recognize the monetary value of users' Personal Information,
2 insofar as they encourage users to install applications explicitly for the purpose of selling that information
3 to technology companies in exchange for monetary benefits.⁴²

4 153. The California Consumer Protection Act ("CCPA") recognizes that consumers' personal
5 data is a property right. Not only does the CCPA prohibit covered businesses from discriminating against
6 consumers that opt-out of data collection, the CCPA also expressly provides that: "[a] business may offer
7 financial incentives, including payments to consumers as compensation, for the collection of personal
8 information, the sale of personal information, or the deletion of personal information." Cal. Civ. Code §
9 1798.125(b)(1). The CCPA provides that, "[a] business shall not use financial incentive practices that are
10 unjust, unreasonable, coercive, or usurious in nature." Cal. Civ. Code § 1798.125(b)(4).

11 **B. Defendants have taken possession of and commercially exploited the personal**
12 **information of plaintiffs and class members without permission and without**
13 **compensation.**

14 154. Defendants have unlawfully taken possession of and commercially exploited the Personal
15 Information of Plaintiffs and Class members without their permission and without compensating them
16 for the use of their assets.

17 155. Defendants' illegal and improper collection, use and retention of children's Personal
18 Information also has given them a significant "first mover" advantage that cannot be undone. TikTok
19 operates one of the most popular apps in the world, and as a result of its unlawful conduct, TikToks's
20 algorithms now incorporate ill-gotten data from millions of children's account. The deep insights gleaned
21 from these viewing sessions will enable TikTok to use the Personal Information of children for potentially
22 the duration of their lives, and will solidify TikToks's dominance in the market for child-related content.

23
24
25 ³⁸ Kari Paul, *Google launches app that will pay users for their data*, The Guardian (June 11, 2019),
26 <https://www.theguardian.com/technology/2019/jun/11/facebook-user-data-app-privacy-studay>; Saheli
27 Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of*
28 *data*, CNBC (Jan. 30, 2019), <https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html>; Jay Peters, *Facebook will now pay you for your voice recordings*, The
Verge (Feb. 20, 2020), <https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-pronunciations-app>.

156. Defendants' exploitation of Plaintiffs' and Class members' Personal Information, without compensation, has caused Plaintiffs and the members of the Classes to suffer economic loss and injury.

157. Defendants' exploitation of Plaintiffs' Class members' Personal Information, without compensation, has caused Plaintiffs Class members to suffer ascertainable losses.

C. The unlawful collection and exploitation of Plaintiffs' and Class members' Personal Information has deprived them of the value of protecting that information from being sold and exploited in the digital information marketplace, and has diminished its value, causing economic loss and injury.

158. Defendants' unlawful collection and commercial exploitation of the Personal Information of Plaintiffs and Class members has deprived Plaintiffs and Class members of the right and privilege of ownership that was most important to them – the right to maintain the privacy of their Personal Information and NOT to sell it. Defendants' conduct has thus destroyed the fundamental quality of the asset and diminished its value to Plaintiffs and the Class members. And, for those Plaintiffs and Class members who would choose to sell their Personal Information in what is a well-established and readily available marketplace, Defendants' conduct has diminished the amount a knowledgeable buyer would be willing to pay for the Information.

159. Once a child's Personal Information has been collected and exploited by Defendants, it is no longer possible for the child or the child's parents to maintain the confidentiality of the data – the aspect of the data that provides the major component of its value to the children and their parents and that, correspondingly, determines the price a seller would be willing to accept – and that a buyer would need to offer – for the data. Researchers have explored the economic implications and market dynamics under such circumstances and have determined that Defendants' conduct thus diminishes the value of the child's Personal Information since a knowledgeable buyer of the data would understand that the data has been deprived of its primary value to the user and would decrease the amount it would be willing to pay – and the amount the user would be willing to accept – for the data.⁴³

⁴³ "Too Much Data: Prices and Inefficiencies in Data Markets," by Daron Acemoglu (MIT), Ali Makhdoumi (Duke University), Azarakhsh Malekian (University of Toronto), and Asu Ozdaglar (MIT),

1 160. The value of the Personal Information of Plaintiffs' and the members of the Classes has
 2 also been diminished by Defendants' wrongful conduct because, as a consequence of gathering the
 3 Personal Information of a massive number of child TikTok users, TikTok has been able to develop large
 4 subsets of TikTok users with correlated interests – *i.e.*, users who share interests in similar (or opposite)
 5 areas and who can be expected to respond similarly to behavioral advertising or to targeted programming.
 6 ⁴⁴ Researchers have also studied the market dynamics in such a scenario for additional members of such
 7 subsets whose preferences correlate with other users in a given subset. ⁴⁵ Because TikTok already
 8 possesses tracking information from other members of the subset sufficient to identify user preferences,
 9 TikTok has less need for the Personal Information of additional subset members and the value of their
 10 Personal Information is, thus, decreased.⁴⁶

11 161. In both of the above scenarios, the desire/willingness of the user to protect his or her data
 12 from exposure is diminished, and the amount of compensation required to cause the user to expose (*i.e.*,
 13 sell) the data – and the amount of a buyer would need to offer -- is diminished. And, because the user's
 14

15
 16
 17 American Economic Journal: Microeconomics, 14(4), 218–256, 2022, <https://www.aeaweb.org/articles?id=10.1257/mic.20200200>, accessed 7/14/24.

18
 19 ⁴⁴ See, e.g., <https://www.indexexchange.com/2023/12/12/google-privacy-sandbox-get-started/>
 20 (accessed 7/14/24), <https://developers.google.com/privacy-sandbox/overview/relevance-and-measurement-faqs> (accessed 7/14/24), and <https://developers.google.com/privacy-sandbox/relevance/protected-audience> (accessed 7/14/24).

21
 22 ⁴⁵ See, e.g., <https://www.indexexchange.com/2023/12/12/google-privacy-sandbox-get-started/>
 23 (accessed 7/14/24), <https://developers.google.com/privacy-sandbox/overview/relevance-and-measurement-faqs> (accessed 7/14/24), and <https://developers.google.com/privacy-sandbox/relevance/protected-audience> (accessed 7/14/24).

24
 25 ⁴⁶ “Too Much Data: Prices and Inefficiencies in Data Markets,” by Daron Acemoglu (MIT), Ali
 26 Makhdoumi (Duke University), Azarakhsh Malekian (University of Toronto), and Asu Ozdaglar (MIT),
 27 American Economic Journal: Microeconomics, 14(4), 218–256, 2022, <https://www.aeaweb.org/articles?id=10.1257/mic.20200200>, accessed 7/14/24. See, also, “Privacy and personal data collection with
 28 information externalities,” by Jay Pil Choi, Doh-Shin Jeon and Byung-Cheol Kim, *Journal of Public Economics*, 173, 113–124, 2019.

1 data is now available to either TikTok or a competitor at a reduced price, the value of the correlated data
2 of all of the other members of the subset is, likewise, diminished.

3 162. For children (or their parents) for whom the sole value of the Personal Information derives
4 from maintaining user privacy, the economic value of the Personal Information has been completely
5 destroyed by Defendants' collection and use of it.

6 163. Defendants' unlawful exploitation of the Personal Information of Plaintiffs and Class
7 members has, thus, diminished the value of their Personal Information, causing Plaintiffs and Class
8 members to suffer economic loss and injury for which Plaintiffs and Class members can never be made
9 whole.

10 164. Defendants' unlawful exploitation of the Personal Information of Plaintiffs and the
11 members of the Classes has, thus, diminished the value of their Personal Information, causing Plaintiffs
12 and the members of the Classes to suffer ascertainable economic loss.

13 **IV. Equitable Relief is Necessary to Protect the Rights of Plaintiffs and the Members of the**
14 **Classes and to Prevent Defendants from Profiting from their Wrongful Conduct.**

15 165. Throughout the Class Period TikTok collected, used and stored COPPA-protected
16 Personal Information from Plaintiffs and Class members without obtaining the verified parental consent
17 required by COPPA for such collection and use.

18 166. TikTok's refusal to abide by the terms of the 2019 Permanent Injunction, as
19 demonstrated by the DOJ's August 2, 2024 Complaint, means that TikTok continues to profit off its
20 unlawful business practices at the expense of the safety and privacy of children. Among other things
21 detailed in the DOJ Complaint, TikTok has failed to implement adequate age gates, to identify and
22 remove underage users of non-Kids Mode accounts, to delete data, even upon parental request, has
23 taken steps to make deletion requests onerous, and has continued to collect data from purportedly
24 deleted accounts.

25 167. Because of TikTok's continued unlawful conduct in collecting and storing the Personal
26 Information of children under the age of 13, Plaintiffs and Class members are not only vulnerable to
27 TikTok's fresh violations, but their previously collected data remains vulnerable to misuse by
28 Defendants. These continuing harms have no adequate remedy at law.

1 168. A.A., A.B., A.C. and Class members are likely to use TikTok in the future and seek
2 protection from Defendants continuing violations of COPPA protections.

3 169. Furthermore, the 2019 Permanent Injunction does not require TikTok to forfeit the
4 profits it realized from its wrongful exploitation of Plaintiffs' and Class members Personal Information,
5 thus allowing TikTok to retain the enormous profits it obtained through its illegal use of Plaintiffs' and
6 Class members' Personal Information. No remedy at law available to Plaintiffs and Class members
7 reaches these profits or is available to prevent TikTok from retaining such profits. The law requires
8 imposition of equitable orders of non-restitutionary disgorgement to prevent TikTok from profiting
9 from their misconduct even without any showing of corresponding economic harm suffered by
10 Plaintiffs and Class members from Defendants' receipt of such profits.

11 170. Money damages will not protect Plaintiffs and the Class members from the non-
12 economic harms discussed herein posed by misuse of their Personal Information collected in violation
13 of COPPA or TikTok's impermissible profit from its misconduct, and Plaintiffs and Class members,
14 thus, have no adequate remedy at law. To the extent that money damages, if available, would
15 constitute an adequate remedy at law barring recovery, Plaintiffs and Class members assert their claims
16 for the equitable relief set forth herein as an alternative remedy pending a final determination of the
17 availability of a remedy at law.

18 171. For these reasons, Plaintiffs and Class members seek entry of a permanent injunction (a)
19 requiring TikTok to destroy all Personal Information of Plaintiffs and Class members in its possession
20 that was collected in violation of COPPA; (b) requiring TikTok to notify each Plaintiff and Class
21 member that his or her Personal Information was collected and has been destroyed; (c) restraining
22 TikTok from directly or indirectly using or benefitting from the Personal Information of Plaintiffs and
23 Class members that it wrongly collected, including precluding the use of any profile of any Plaintiff or
24 Class member developed in whole or in part based on such information in serving targeted or
25 behavioral advertising; and (d) requiring TikTok's relinquishment of all ill-gotten gains.

ALLEGATIONS RELATING TO PLAINTIFFS

A. Plaintiff A.A.

172. During the Class Period, Plaintiff A.A. had a TikTok account, which A.A. transferred from a Musical.ly account.

173. When A.A. interacted with TikTok (formerly Musical.ly), Defendants collected the Personal Information of A.A. for the purpose of tracking, profiling, and targeting A.A. with curated content and advertisements.

174. Defendants did not provide notification or obtain verifiable consent from A.A.'s parent and guardian, Marcelo Muto, prior to collecting A.A.'s Personal Information.

175. Neither A.A. nor their parent and guardian could have reasonably discovered this conduct earlier through investigation as Defendants purported to be abiding by a Permanent Injunction designed to prohibit this conduct throughout the Class Period.

176. A.A. is likely to use TikTok in the future and seeks protection from Defendants continuing violations of COPPA protections.

D. Plaintiff A.B.

177. During the Class Period, Plaintiff A.B. had a TikTok account.

178. When A.B. interacted with TikTok, Defendants collected the Personal Information of A.B. for the purpose of tracking, profiling, and targeting A.B. with curated content and advertisements.

179. Defendants did not provide notification or obtain verifiable consent from A.B.'s parent and guardian, Heather Bressette, prior to collecting A.B.'s Personal Information.

180. Neither A.B. nor their parent and guardian could have reasonably discovered this conduct earlier through investigation as Defendants purported to be abiding by a Permanent Injunction designed to prohibit this conduct throughout the Class Period.

181. A.B. is likely to use TikTok in the future and seeks protection from Defendants continuing violations of COPPA protections.

E. Plaintiff A.C.

182. During the Class Period, Plaintiff A.C. had a TikTok account.

183. When A.C. interacted with TikTok, Defendants collected the Personal Information of A.C. for the purpose of tracking, profiling, and targeting A.C. with curated content and advertisements.

184. Defendants did not provide notification or obtain verifiable consent from A.C.'s parent and guardian, Darryl Maultsby, prior to collecting A.C.'s Personal Information.

185. Neither A.C. nor their parent and guardian could have reasonably discovered this conduct earlier through investigation as Defendants purported to be abiding by a Permanent Injunction designed to prohibit this conduct throughout the Class Period.

186. A.C. is likely to use TikTok in the future and seeks protection from Defendants continuing violations of COPPA protections.

TOLLING, ESTOPPEL AND RELATION BACK

I. Discovery Rule Tolling

187. Plaintiffs and the Classes had no way of knowing about Defendants' conduct with respect to the collection and impermissible and unauthorized use of, and profit from, the Personal Information of Plaintiffs and the members of the Classes.

188. Neither Plaintiffs nor any other members of the Classes, through the exercise of reasonable diligence, could have discovered the conduct alleged herein as Defendants purported to be abiding by the terms of a Permanent Injunction that prohibited the subject conduct. Further, Plaintiffs and the members of the Classes did not discover and did not know of facts that would have caused a reasonable person to suspect, that Defendants were engaged in the conduct alleged herein.

189. For these reasons, all applicable statutes of limitation have been tolled by operation of the discovery rule with respect to claims asserted by Plaintiffs and the Classes.

II. Fraudulent Concealment Tolling

190. By failing to provide notice of the collection and use of the Personal Information and obtain verifiable consent, in violation of COPPA and societal norms and conventions, Defendants concealed their conduct and the existence of the claims asserted herein from Plaintiffs and the members of the Classes.

191. Upon information and belief, Defendants intended by their acts to conceal the facts and claims from Plaintiffs and members of the Classes. Plaintiffs and the members of the Classes were

unaware of the facts alleged herein without any fault or lack of diligence on their part and could not have reasonably discovered Defendants' conduct. For this reason, any statute of limitations that otherwise may apply to the claims of Plaintiffs or members of the Classes should be tolled.

III. Estoppel

192. Despite their duties and obligations under COPPA and the 2019 Permanent Injunction, Defendants failed to provide notice of the collection and use of the Personal Information and obtain verifiable consent in breach and violation thereof.

193. Defendants therefore are estopped from relying on any statutes of limitations in defense of this action.

CLASS ACTION ALLEGATIONS

194. Plaintiffs bring this action as a class action pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3).

I. The California Class

195. Plaintiff A.A., through their parent and guardian Marcelo Muto, seeks class certification of a claim for violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*, a claim for violation of the State of California Constitution Right to Privacy, for the common law claim of intrusion upon seclusion, as well as a claim for unjust enrichment on behalf of a California class defined as follows:

All persons residing in the State of California who were 13 or younger when they used TikTok, and from whom Defendants collected, caused to be collected, used, or disclosed Personal Information without first obtaining verified parental consent during the Class Period.

II. The Connecticut Class

196. Plaintiff L.F, through their parent and guardian Heather Bressette, seeks class certification for the violation of Connecticut Unfair Trade Practices Act, CONN. GEN. STAT. § 42-110b(a), *et seq.*, common law claim of intrusion upon seclusion, as well as a claim for unjust enrichment on behalf of a Connecticut class defined as follows:

All persons residing in the State of Connecticut who were 13 or younger when they used TikTok, and from whom Defendants collected, caused to be collected, used, or disclosed Personal Information without first obtaining verified parental consent during the Class Period.

1 **III. The Florida Class**

2 197. Plaintiff A.C., through their parent and guardian Darryl Maulsby, seeks class
3 certification for the violation of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. §
4 501.201 *et seq.*, and unjust enrichment on behalf of a Florida class defined as follows:

5 All persons residing in the State of Florida who were 13 or younger when they used
6 TikTok, and from whom Defendants collected, caused to be collected, used, or
7 disclosed Personal Information without first obtaining verified parental consent
8 during the Class Period.

9 198. Plaintiffs reserve the right to modify or refine the Class definitions based upon discovery
10 of new information and in order to accommodate any of the Court's manageability concerns.

11 199. Excluded from the Classes are: (a) any Judge or Magistrate Judge presiding over this
12 action and members of their staff, as well as members of their families; (b) Defendants and Defendants'
13 predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or
14 its parents have a controlling interest, as well as Defendants' current or former employees, agents,
15 officers, and directors; (c) persons who properly execute and file a timely request for exclusion from the
16 Classes; (d) persons whose claims in this matter have been finally adjudicated on the merits or otherwise
17 released; (e) counsel for Plaintiffs and Defendants; and (f) the legal representatives, successors, and
18 assigns of any such excluded persons.

19 200. **Ascertainability.** The proposed Classes are readily ascertainable because they are
20 defined using objective criteria so as to allow class members to determine if they are part of a Class.
21 Further, the Classes can be identified through records maintained by Defendants.

22 201. **Numerosity (Rule 23(a)(1)).** The Classes are so numerous that joinder of individual
23 members herein is impracticable. The exact number of members of the Classes, as herein identified and
24 described, is not known, but all public estimates confirm that TikTok has collected information on
25 millions of children.

26 202. **Commonality (Rule 23(a)(2)).** Common questions of fact and law exist for each cause
27 of action and predominate over questions affecting only individual Class members, including the
28 following:

a. Whether Defendants collected the Personal Information of children;

- b. Whether Defendants had knowledge they were collecting the Personal Information of children;
- c. Whether Defendants obtained parental consent to collect the Personal Information of children;
- d. Whether the collection of Personal Information of children is highly offensive to a reasonable person;
- e. Whether the collection of Personal Information of children without parental consent is sufficiently serious and unwarranted as to constitute an egregious breach of social norms;
- f. Whether Defendants' conduct constituted an invasion of privacy based on common law protection against intrusion upon seclusion under the laws of California and Connecticut.
- g. Whether Defendants' conduct constituted a violation of the California Constitution right to privacy;
- h. Whether Defendants' conduct was unfair;
- i. Whether Defendants' conduct was unlawful;
- j. Whether Defendants' conduct violated the consumer protection acts of California, Connecticut and Florida;
- k. Whether Plaintiffs and the Classes are entitled to monetary damages and the measure of those damages;
- l. Whether the California Class is entitled to restitution and disgorgement;
- m. Whether Defendants were unjustly enriched by their conduct under the laws of California, Connecticut, and Florida;
- n. Whether Defendants fraudulently concealed their conduct; and
- o. Whether Plaintiffs and the Classes are entitled to injunctive or other equitable relief.

203. **Typicality (Rule 23(a)(3)).** Plaintiffs' claims are typical of the claims of the other members of the proposed Classes. Plaintiffs and members of the Classes (as applicable) suffered an

1 invasion of privacy and injuries as a result of Defendants' wrongful conduct that is uniform across the
2 Classes.

3 204. **Adequacy (Rule 23(a)(4)).** Plaintiffs have and will continue to fairly and adequately
4 represent and protect the interests of the Classes. Plaintiffs have retained counsel competent and
5 experienced in complex litigation and class actions. Plaintiffs have no interest that is antagonistic to
6 those of the Classes, and Defendants have no defenses unique to Plaintiffs. Plaintiffs and their counsel
7 are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they
8 have the resources to do so. Neither Plaintiffs nor Plaintiffs' counsel have any interest adverse to those
9 of the other members of the Classes.

10 205. **Substantial Benefits.** This class action is appropriate for certification because class
11 proceedings are superior to other available methods for the fair and efficient adjudication of this
12 controversy and joinder of all members of the Classes is impracticable. The prosecution of separate
13 actions by individual members of the Classes would impose heavy burdens upon the Courts and
14 Defendants, would create a risk of inconsistent or varying adjudications of the questions of law and fact
15 common to members of the Classes, and would be dispositive of the interests of the other members not
16 parties to the individual adjudications or would substantially impair or impede their ability to protect
17 their interests. This proposed class action presents fewer management difficulties than individual
18 litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive
19 supervision by a single court. Class treatment will create economies of time, effort, and expense and
20 promote uniform decision-making.

21 206. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3) because the
22 above common questions of law or fact predominate over any questions affecting individual members
23 of the Classes, and a class action is superior to other available methods for the fair and efficient
24 adjudication of this controversy.

25 207. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants
26 have acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief
27 or corresponding declaratory relief, if any, that may be awarded by the Court is appropriate as to the
28 Classes as a whole.

208. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CLAIMS FOR RELIEF

I. CALIFORNIA CLAIMS

Claim 1

CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY, Cal. Const. Art. 1, § 1. (Against All Defendants on behalf of Plaintiff A.A. and the California Class)

209. Plaintiff A.A., and members of the California Class re-allege the foregoing allegations as if fully set forth herein.

210. A.A. and members of the California Class's private affairs include their behavior on their mobile devices and computers, as well as any other behavior that may be monitored by the surreptitious tracking employed or otherwise enabled by Defendants.

211. The parents and guardians of A.A. and members of the California Class have reasonable expectations of privacy in their children's mobile devices and their online behavior and activities, generally.

212. A.A. and members of the California Class's private affairs, concerns, and seclusion includes their interest in their Personal Information as defined by COPPA, which includes data points concerning their location and online activity while using internet-connected devices.

213. Defendants intentionally intruded upon the private affairs, concerns, and seclusion of A.A. and California Class members by improperly accessing A.A. and California Class members' Personal Information and using it for improper purposes, including by targeting them with behavioral advertising that would be highly offensive to a reasonable person, constituting an egregious breach of social norms and/or enabling the targeting of A.A. and California Class members with such advertisements, as detailed herein.

214. Defendants' intrusions upon the private affairs, concerns, and seclusion of A.A. and California Class members were substantial, and would be highly offensive to a reasonable person, constituting an egregious breach of social norms, as is evidenced by consumer surveys, and academic studies detailing the harms of tracking children online, centuries of common law, state and federal statutes

1 and regulations including COPPA and FTC regulations, legislative commentaries, enforcement actions
 2 undertaken by the FTC, industry standards and guidelines, scholarly literature on consumers' reasonable
 3 expectations, the fines imposed on TikTok by the FTC, as well as the reforms required by the 2019
 4 Permanent Injunction entered into by TikTok, which it has now been accused of violating.

5 215. As minor children, A.A. and members of the California Class lacked the ability to form
 6 expectations about reasonable privacy or to consent to Defendants' actions.

7 216. Neither A.A., members of the California Class, nor their parents and/or guardians
 8 consented to Defendants' intrusions upon their private affairs, concerns, and seclusions.

9 217. A.A. and members of the California Class suffered actual and concrete injury as a result
 10 of Defendants' intrusions upon Plaintiffs' private affairs, concerns, and seclusion.

11 218. A.A. and members of the California Class seek appropriate relief for that injury, including
 12 but not limited to damages that will reasonably compensate them for the harm to their privacy interests,
 13 risk of future invasions of privacy, and the mental and emotional distress caused by Defendants' invasions
 14 of privacy, as well as disgorgement of profits made by Defendants as a result of their intrusions upon
 15 A.A. and members of the California Class's private affairs, concerns, and seclusion.

16 **Claim 2**

17 **CALIFORNIA INTRUSION UPON SECLUSION** 18 **(Against All Defendants on behalf of Plaintiff A.A. and the California Class)**

19 219. Plaintiff A.A. and members of the California Class re-allege the foregoing allegations as
 20 if fully set forth herein.

21 220. A.A. and members of the California Class's private affairs, concerns, and seclusion
 22 includes their interest in their Personal Information as defined by COPPA, which includes data points
 23 concerning their location and online activity while using internet-connected devices.

24 221. Defendants intentionally intruded upon the private affairs, concerns, and seclusion of A.A.
 25 and California Class members by improperly accessing A.A. and California Class members' Personal
 26 Information and using it for improper purposes, including by targeting them with behavioral advertising
 27 that would be highly offensive to a reasonable person, constituting an egregious breach of social norms
 28

1 and/or enabling the targeting of A.A. and California Class members with such advertisements, as detailed
2 herein.

3 222. Defendants' intrusions upon the private affairs, concerns, and seclusion of A.A. and
4 California Class members were substantial, and would be highly offensive to a reasonable person,
5 constituting an egregious breach of social norms, as is evidenced by countless consumer surveys, and
6 academic studies detailing the harms of tracking children online, centuries of common law, state and
7 federal statutes and regulations including COPPA and FTC regulations, legislative commentaries,
8 enforcement actions undertaken by the FTC, industry standards and guidelines, scholarly literature on
9 consumers' reasonable expectations, the fines imposed on TikTok by the FTC, as well as the reforms
10 required by the 2019 Permanent Injunction entered into by TikTok, which it has now been accused of
11 violating.

12 223. As minor children, A.A. and members of the California Class lacked the ability to form
13 expectations about reasonable privacy or to consent to Defendants' actions.

14 224. Neither A.A., members of the California Class, nor their parents and/or guardians
15 consented to Defendants' intrusions upon their private affairs, concerns, and seclusions.

16 225. A.A. and members of the California Class suffered actual and concrete injury as a result
17 of Defendants' intrusions upon A.A. and California Class members' private affairs, concerns, and
18 seclusion.

19 226. A.A. and members of the California Class seek appropriate relief for that injury, including
20 but not limited to damages that will reasonably compensate them for the harm to their privacy interests,
21 risk of future invasions of privacy, and the mental and emotional distress caused by Defendants' invasions
22 of privacy, as well as disgorgement of profits made by Defendants as a result of their intrusions upon
23 B.M and members of the California Class's private affairs, concerns, and seclusion.

Claim 3

**CALIFORNIA UNFAIR COMPETITION LAW (UCL),
Cal. Bus. & Prof. Code § 17200, *et seq.*
(Against All Defendants on behalf of Plaintiff A.A. and the California Class)**

227. Plaintiff A.A. and members of the California Class incorporate the foregoing allegations as if fully set forth herein.

228. A.A. and members of the California Class are or were residents of California and/or engaged with the TikTok in California.

229. At all times mentioned herein, Defendants each engaged in “trade” or “commerce” in California in that they each engaged in the advertising, offering for sale, sale, and distribution of property or any other articles, commodities, or things of value in California.

230. Defendants each engaged in consumer-oriented acts through the offering, promotion, and/or distribution of the TikTok, which significantly impacted the public because TikTok is used nationwide, including in California, and there are millions of users, including A.A. and members of the California Class.

231. Cal. Bus. & Prof. Code § 17200, *et seq.* (the “UCL”) broadly prohibits “unfair competition”, which the UCL defines as including “any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising[.]”

232. California courts have noted that “the differences [between the UCL and FTC Act] are not of a degree to impair comparison” and that unfair acts respectively proscribed in the two statutes “appear practically synonymous.” *People ex rel. Mosk v. Nat’l Rsch. Co. of Cal.*, 201 Cal. App. 2d 765, 773, 20 Cal. Rptr. 516, 521 (Ct. App. 1962). As a result, California courts deem “decisions of the federal court [construing the FTC Act] are more than ordinarily persuasive.” *Id.*

233. Defendants violated Cal. Bus. & Prof. Code § 17200, *et seq.* by engaging in the unfair acts or practices proscribed by Cal. Bus. & Prof. Code § 17200, *et seq.* outlined herein.

234. Defendants at all relevant times knowingly violated legal duties and public policy by unfairly and unlawfully collecting the Personal Information of minor children and tracking, profiling, and targeting those children with behavioral advertising for Defendants’ commercial financial gain.

1 235. As outlined herein, Defendants at all times had actual knowledge of their own non-
2 compliance with COPPA and other applicable privacy-related laws. Further, Defendants at all times had
3 actual knowledge of their own collection of the Personal Information from A.A. and California Class
4 members and the tracking, profiling, and targeting of those children for lucrative behavioral advertising.

5 236. As outlined herein, Defendants intentionally designed TikTok to, among other things,
6 attract minor children by making child-directed content available to them so that TikTok could collect
7 the Personal Information of those children for substantial commercial gain.

8 237. TikTok was aware at all times that a significant portion of its users were under the age of
9 13 and nonetheless collected the Personal Information of those children for the purpose of serving those
10 children behavioral advertising for substantial commercial gain. After entering into a Permanent
11 Injunction with the United States in 2019 intended to prohibit Defendants from their continued collection
12 or use of the Personal Information of children under the age of 13, Defendants purposefully sought to
13 undermine their compliance through, among other practices, implementation of a woefully inadequate
14 age-gating system, and monitoring policies and procedures designed to allow them to continue knowingly
15 collecting and using the Personal Information of children.

16 238. Defendants are considered by the FTC to be “operators” as defined under COPPA and
17 FTC regulations.

18 239. In particular, Defendants systematically collected, used, and/or disclosed Personal
19 Information from minor children in violation of COPPA, and therefore the FTC Act, to serve them
20 targeted, behavioral advertising by inter alia:

- 21 a. Failing to provide sufficient notice of the information Defendants collected, or the
22 information that was collected on Defendants’ behalf, online from children under
23 13, how Defendants used such information, their disclosure practices, and all other
24 required content, in violation of Section 312.4(d) of COPPA, 16 C.F.R. § 312.4(d);
25 b. Failing to provide direct notice to parents of the information Defendants collected,
26 or the information that was collected on Defendants’ behalf, online from children
27 under 13, how Defendants used such information, their disclosure practices, and
28

all other required content, in violation of Section 312.4(b) and (c) of COPPA, 16 C.F.R. § 312.4(b)-(c);

c. Failing to obtain verifiable parental consent before any collection or use of Personal Information from children under 13, in violation of Section 312.5 of COPPA, 16 C.F.R. § 312.5; and

d. Failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information collected from children under 13, in violation of Section 312.8 of COPPA, 16 C.F.R. § 312.8.

240. Violations of COPPA and the accompanying FTC regulations “shall be treated as a violation of a rule defining an unfair ... act or practice prescribed under 15 U.S.C. § 57a(a)(1)(B).” 15 U.S.C. § 6502(c). These rules define unfair acts or practices in or affecting commerce within the meaning of 15 U.S.C. § 45(a)(1), which is the model for the various consumer protection statutes in the several states, including the Cal. Bus. & Prof. Code § 17200, *et seq.*⁴⁷

241. Accordingly, Defendants engaged in unfair and unlawful trade acts or practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq.*, which is modeled after, proscribes the same conduct as, and gives deference to the definitions of the FTC Act.

242. Defendants’ conduct is unfair, immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, and there are no greater countervailing benefits to consumers or competition. Further, A.A. and members of the California Class could not have reasonably avoided injury because Defendants each took advantage of the lack of knowledge, ability, experience, and/or capacity of consumers—in this case children under 13—to their detriment.

243. Defendants willfully engaged in the unfair and unlawful acts described herein and knew or recklessly disregarded the fact that they violated Cal. Bus. & Prof. Code § 17200, *et seq.*

⁴⁷ See 16 C.F.R. § 312.1 (COPPA “prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure or personal information from and about children on the internet.”).

1 244. A.A. and members of the California Class were harmed by Defendants' practices
2 described herein, which were a substantial factor and caused injury in fact and actual damages to A.A.
3 and members of the California Class.

4 245. As a direct and proximate result of Defendants' unfair and unlawful acts and practices in
5 violation of Cal. Bus. & Prof. Code § 17200, *et seq.*, C.H. and members of the California Class have
6 suffered and will continue to suffer an ascertainable loss of money or property, real or personal, and
7 monetary and non-monetary damages, as described herein, including, inter alia, the loss of the value
8 and/or diminishment in value of their Personal Information and the loss of the ability to control the use
9 of their Personal Information.

10 246. As outlined herein, there is tangible value in A.A. and members of the California Class's
11 Personal Information. A.A. and members of the California class have lost the opportunity to receive value
12 in exchange for their Personal Information.

13 247. Defendants' monetization of A.A. and members of the California Class's Personal
14 Information demonstrates that there is a market for their Personal Information.

15 248. A.A. and members of the California Class's Personal Information is now in the possession
16 of Defendants, who have used and will use it for their financial gain.

17 249. Defendants' retention of A.A. and members of the California Class's Personal Information
18 presents a continuing risk to them as well as the general public. A.A. and members of the California Class
19 seek relief for the injuries they have suffered as a result of Defendants' unfair and unlawful acts and
20 practices, as provided by Cal. Bus. & Prof. Code § 17200, *et seq.* and applicable law, including all actual
21 damages and attorneys' fees and costs, treble damages, statutory damages, and restitution, as well as an
22 injunction requiring Defendants to permanently delete, destroy or otherwise sequester the Personal
23 Information collected without parental consent, requiring Defendants to provide a complete audit and
24 accounting of the uses of the Personal Information by them and any other third parties, and other
25 appropriate injunctive and/or declaratory relief.
26
27
28

Claim 4

California Unjust Enrichment

(Against All Defendants on behalf of A.A. and members of the California Class)

250. Plaintiff A.A. and members of the California Class incorporate and reallege all allegations set forth above.

251. By virtue of the unlawful and unfair conduct alleged herein, Defendants have realized millions of dollars in revenue from their collection and use of the Personal Information of A.A. and the California Class members through behavioral advertising and commercialization of Plaintiffs' Personal Information.

252. Defendants' ill-gotten gains were monetary benefits conferred upon Defendants by A.A. and the members of the California Class. It would be inequitable and unjust to permit any of the Defendants to retain the economic benefits they have obtained through advertising and commercialization derived from the Personal Information of A.A. and the members of the California Class.

253. Defendants will be unjustly enriched if they are permitted to retain the economic benefits conferred upon them by A.A. and the members of the California Class through their unlawful, unfair, unauthorized, and impermissible use of the Personal Information of A.A. and members of the California Class, and allowing Defendants to retain the profits from their unlawful, unauthorized, and impermissible use of the Personal Information of A.A. and the members of the California Class would be unjust and contrary to public policy.

254. A.A. and the members of the California Class are therefore entitled to recover the amounts realized by the Defendants at the expense of A.A. and the members of the California Class.

255. A.A. and members of the California Class do not seek recover in this claim for their own economic harm and have no adequate remedy at law that would divest Defendants of their ill-gotten and unjust profits. To the extent that money damages, if available, would constitute an adequate remedy at law barring recovery under this claim, A.A. and members of the California Class assert their claim for non-restitutionary disgorgement as an alternative remedy.

256. A.A. and members of the California Class are entitled to non-restitutionary disgorgement of Defendants' ill-gotten gains, and/or the imposition of a constructive trust to recover the amount of Defendants' ill-gotten gains.

II. CONNECTICUT CLAIMS

Claim 5

**FOR DECEPTIVE AND UNFAIR PRACTICES IN VIOLATION OF
THE CONNECTICUT UNFAIR TRADE PRACTICES ACT,
CONN. GEN. STAT. § 42-110a, *ET SEQ.*
(Against all Defendants on behalf of Plaintiff A.B. and the Connecticut Class)**

257. Plaintiffs reallege the allegations set forth in IV, V(d), and XII above.

258. This claim is asserted against Defendants pursuant to Conn. Gen. Stat. § 42-110a, *et. seq.*

259. The Connecticut Unfair Trade Practices Act (CUTPA), Conn. Gen. Stat. § 42-110a, *et seq.*, declares that “unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful.”

260. Pursuant to Conn. Gen. Stat. § 42-110g(a), any person who has suffered a loss as a result of a violation of CUTPA may bring an action to obtain a declaratory judgment that an act or practice violates CUTPA and to enjoin such person who has violated, is violating, or is otherwise likely to violate CUTPA.

261. Pursuant to Conn. Gen. Stat. § 42-110g(a), any person who has suffered a loss as a result of a violation of CUTPA may bring an action for actual damages, attorneys’ fees, and court costs.

262. Plaintiffs and Defendants are each a “person” within the meaning of Conn. Gen. Stat. § 42-110a(3).

263. Defendants through their conduct as described above, engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of their trade and commerce, as defined in General Statutes § 42-110a(4), within the State of Connecticut.

264. Connecticut courts have held that “it is the intent of the legislature that in construing subsection (a) of this section, the commissioner [of consumer protection] and the courts of this state shall be guided by interpretations given by the Federal Trade Commission and the federal courts to Section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)).” *Heslin v. Connecticut L. Clinic of Trantolo & Trantolo*, 190 Conn. 510, 518, 461 A.2d 938, 942 (1983) as from time to time amended.”

1 265. Defendants at all relevant times knowingly violated legal duties and public policy by
2 unfairly and unlawfully collecting the Personal Information of minor children and tracking, profiling,
3 and targeting those children with behavioral advertising for Defendants' commercial financial gain.

4 266. As outlined herein, Defendants at all times had actual knowledge of their non-
5 compliance with COPPA and other applicable privacy-related laws. Further, Defendants at all times
6 had actual knowledge of their own collection of the Personal Information from A.B. and Connecticut
7 Class members and the tracking, profiling, and targeting of those children for lucrative behavioral
8 advertising.

9 267. As outlined herein, Defendants intentionally designed TikTok to, among other things,
10 attract minor children by making child-directed content available to them so that TikTok could collect
11 the Personal Information of those children for substantial commercial gain.

12 268. TikTok was aware at all times that a significant portion of its users were under the age of
13 13 and nonetheless collected the Personal Information of those children for the purpose of serving those
14 children behavioral advertising for substantial commercial gain. After entering into a Permanent
15 Injunction with the United States in 2019 intended to prohibit Defendants from their continued collection
16 or use of the Personal Information of children under the age of 13, Defendants purposefully sought to
17 undermine their compliance through, among other practices, implementation of a woefully inadequate
18 age-gating system, and monitoring policies and procedures designed to allow them to continue knowingly
19 collecting and using the Personal Information of children.

20 269. Defendants are considered by the FTC to be "operators" as defined under COPPA and
21 FTC regulations.

22 270. In particular, Defendants systematically collected, used, and/or disclosed Personal
23 Information from minor children in violation of COPPA, and therefore the FTC Act, to serve them
24 targeted, behavioral advertising by inter alia:

- 25 a. Failing to provide sufficient notice of the information Defendants collected, or the
26 information that was collected on Defendants' behalf, online from children under
27 13, how Defendants used such information, their disclosure practices, and all other
28 required content, in violation of Section 312.4(d) of COPPA, 16 C.F.R. § 312.4(d);

- b. Failing to provide direct notice to parents of the information Defendants collected, or the information that was collected on Defendants' behalf, online from children under 13, how Defendants used such information, their disclosure practices, and all other required content, in violation of Section 312.4(b) and (c) of COPPA, 16 C.F.R. § 312.4(b)-(c);
- c. Failing to obtain verifiable parental consent before any collection or use of Personal Information from children under 13, in violation of Section 312.5 of COPPA, 16 C.F.R. § 312.5; and
- d. Failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of Personal Information collected from children under 13, in violation of Section 312.8 of COPPA, 16 C.F.R. § 312.8.

271. Violations of COPPA and the accompanying FTC regulations "shall be treated as a violation of a rule defining an unfair ... act or practice prescribed under 15 U.S.C. § 57a(1)(B)." 15 U.S.C. § 6502(c). These rules define unfair acts or practices in or affecting commerce within the meaning of 15 U.S.C. § 45(a)(1), which is the model for the various consumer protection statutes in the several states, including Conn. Gen. Stat. § 42-110a, *et seq.*

272. Accordingly, Defendants engaged in unfair and unlawful trade acts or practices in violation of Conn. Gen. Stat. § 42-110a, *et seq.* which is modeled after, proscribes the same conduct as, and gives deference to the definitions of the FTC Act.

273. Because Defendants knew or should have known that their conduct was deceptive and/or unfair under Conn. Gen. Stat. § 42-110b(a), their conduct was willful under Conn. Gen. Statutes § 42-110o.

274. These unfair and deceptive acts and practices have caused Plaintiffs and other similarly situated consumers and/or businesses to suffer losses of money and property.

275. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs and other similarly situated consumers and/or businesses have suffered damages and are entitled to relief under CUTPA, including, but not limited to, actual damages, attorneys' fees, and costs.

276. Accordingly, Plaintiffs, individually and on behalf of all others similarly situated, thus seek (a) a declaration that Defendants' acts and practices as described above violate the Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110a, *et seq.*; (b) an award of actual damages; (c) an award of attorneys' fees and costs pursuant to Conn. Gen. Stat. § 42-110g(d); (d) an order enjoining Defendants from continuing to engage in the unfair and deceptive acts and practices described above; and any further relief the Court deems just and proper.

Claim 6

CONNECTICUT INTRUSION UPON SECLUSION (Against All Defendants on behalf of Plaintiff A.B. and the Connecticut Class)

277. Plaintiff A.B. and members of the Connecticut Class re-allege the foregoing allegations as if fully set forth herein.

278. A.B. and members of the Connecticut Class's private affairs, concerns, and seclusion includes their interest in their Personal Information as defined by COPPA, which includes data points concerning their location and online activity while using internet-connected devices.

279. Defendants each and in concert, through aid or assistance, or pursuant to a common purpose with the knowledge of the others, intentionally intruded upon the private affairs, concerns, and seclusion of A.B. and Connecticut Class members by improperly accessing A.B. and Connecticut Class members' Personal Information and using it for improper purposes, including by targeting them with behavioral advertising that would be highly offensive to a reasonable person, constituting an egregious breach of social norms and/or enabling the targeting of A.B. and Connecticut Class members with such advertisements, as detailed herein.

280. Defendants' intrusions upon the private affairs, concerns, and seclusion of A.B. and Connecticut Class members were substantial, and would be highly offensive to a reasonable person, constituting an egregious breach of social norms, as is evidenced by countless consumer surveys, and academic studies detailing the harms of tracking children online, centuries of common law, state and federal statutes and regulations including COPPA and FTC regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, scholarly literature on

1 consumers' reasonable expectations, the fines imposed on TikTok by the FTC, as well as the reforms
 2 required by the 2019 Permanent Injunction entered into by TikTok, which it has now been accused of
 3 violating.

4 281. As minor children, A.B. and members of the Connecticut Class lacked the ability to form
 5 expectations about reasonable privacy or to consent to Defendants' actions.

6 282. Neither A.B., nor members of the Connecticut Class, nor their parents and/or guardians
 7 consented to Defendants' intrusions upon their private affairs, concerns, and seclusions.

8 283. A.B. and members of the Connecticut Class suffered actual and concrete injury as a result
 9 of Defendants' intrusions upon A.B. and the Connecticut Class members' private affairs, concerns, and
 10 seclusion.

11 284. A.B., and members of the Connecticut Class seek appropriate relief for that injury,
 12 including but not limited to damages that will reasonably compensate them for the harm to their privacy
 13 interests, risk of future invasions of privacy, and the mental and emotional distress caused by Defendants'
 14 invasions of privacy, as well as disgorgement of profits made by Defendants as a result of their intrusions
 15 upon A.B., and members of the Connecticut class's private affairs, concerns, and seclusion.

16 **Claim 7**

17 **CONNECTICUT UNJUST ENRICHMENT** 18 **(Against All Defendants on behalf of Plaintiff A.B. and the Connecticut Class)**

19 285. Plaintiff A.B., and members of the Connecticut Class re-allege the foregoing allegations
 20 as if fully set forth herein.

21 286. By virtue of the unlawful and unfair conduct alleged herein, Defendants have each realized
 22 millions of dollars in revenue from their collection and use of the Personal Information of A.B. and
 23 Connecticut Class members through behavioral advertising and commercialization purposes derived
 24 from that Personal Information.

25 287. Defendants' ill-gotten gains were monetary benefits conferred upon Defendants by A.B.
 26 and members of the Connecticut Class. It would be inequitable and unjust to permit any of the Defendants
 27 to retain the economic benefits they have obtained through advertising and commercialization derived
 28 from the Personal Information of A.B. and members of the Connecticut Class.

288. Defendants will be unjustly enriched if they are permitted to retain the economic benefits conferred upon them by A.B. and members of the Connecticut Class through their unlawful, unfair, unauthorized, and impermissible use of the Personal Information A.B. and members of the Connecticut Class, and allowing Defendants to retain the profits from their unlawful, unfair, unauthorized, and impermissible use of the Personal Information of A.B. and members of the Connecticut Class would be unjust and contrary to public policy.

289. A.B. and members of the Connecticut Class are therefore entitled to recover the amounts realized by each of the Defendants at the expense of A.B. and members of the Connecticut Class.

290. A.B. and members of the Connecticut Class do not seek recovery in this claim for their own economic harm and have no adequate remedy at law that would divest Defendants of their ill-gotten and unjust profits. To the extent that money damages, if available, would constitute an adequate remedy at law barring recovery under this claim, A.B. and members of the Connecticut Class assert their claim for non-restitutionary disgorgement as an alternative remedy pending a final determination of the availability of a remedy at law.

291. A.B. and members of the Connecticut Class are entitled to non-restitutionary disgorgement of each Defendant's ill-gotten gains, and/or the imposition of a constructive trust to recover the amount of each Defendant's ill-gotten gains.

III. FLORIDA CLAIMS

Claim 8

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT (FDUTPA), Fla. Stat. Ann. § 501.201 *et seq.* (Against All Defendants on behalf of Plaintiff A.C. and the Florida Class)

292. Plaintiff A.C. and members of the Florida Class incorporate the foregoing allegations as if fully set forth herein.

293. A.C. and members of the Florida Class are or were residents of Florida and used TikTok while under the age of 13.

1 294. At all times mentioned herein, Defendants each engaged in “trade” or “commerce” in
2 Florida in that Defendants each engaged in the advertising, offering for sale, sale, and distribution of
3 property or any other articles, commodities, or things of value in Florida.

4 295. Defendants each engaged in consumer-oriented acts through the offer, promotion, and/or
5 distribution of the TikTok app, which significantly impacted the public because TikTok is used
6 nationwide, including in Florida, and there are millions of users, including A.C. and members of the
7 Florida Class.

8 296. Fla. Stat. Ann. § 501.204(1) provides “[u]nfair methods of competition, unconscionable
9 acts or practices, and unfair ... acts or practices in the conduct of any trade or commerce are hereby
10 declared unlawful.”

11 297. Defendants violated Fla. Stat. Ann. § 501.204 by engaging in the deceptive or unfair acts
12 or practices proscribed by Fla. Stat. Ann. § 501.204 outlined herein.

13 298. As outlined herein, Defendants at all times had actual knowledge of their own non-
14 compliance with COPPA and other applicable privacy-related laws. Further, Defendants at all times had
15 actual knowledge of their collection of the Personal Information of A.C. and Florida Class members and
16 the tracking, profiling, and targeting of those children for lucrative behavioral advertising.

17 299. As outlined herein, Defendants intentionally designed TikTok to, among other things,
18 attract minor children by making child-directed content available to them so that TikTok could collect
19 the Personal Information for substantial commercial gain.

20 300. TikTok was aware at all times that a significant portion of its users were under the age of
21 13 and nonetheless collected the Personal Information of those children for the purpose of serving those
22 children behavioral advertising for substantial commercial gain. After entering into a Permanent
23 Injunction with the United States in 2019 intended to prohibit Defendants from their continued collection
24 or use of the Personal Information of children under the age of 13, Defendants purposefully sought to
25 undermine their compliance through, among other practices, implementation of a woefully inadequate
26 age-gating system, and monitoring policies and procedures designed to allow them to continue knowingly
27 collecting and using the Personal Information of children.
28

1 301. In particular, systematically collected, used, and/or disclosed Personal Information from
2 children under 13 in violation of COPPA, and therefore the FTC Act, by:

- 3 a. Failing to provide sufficient notice of the information Defendants collected, or the
4 information that was collected on Defendants' behalf, online from children under
5 13, how Defendants used such information, their disclosure practices, and all other
6 required content, in violation of Section 312.4(d) of COPPA, 16 C.F.R. § 312.4(d);
7 b. Failing to provide direct notice to parents of the information Defendants collected,
8 or the information that was collected on Defendants' behalf, online from children
9 under 13, how Defendants used such information, their disclosure practices, and
10 all other required content, in violation of Section 312.4(b) and (c) of COPPA, 16
11 C.F.R. § 312.4(b)-(c);
12 c. Failing to obtain verifiable parental consent before any collection or use of
13 Personal Information from children under 13, in violation of Section 312.5 of
14 COPPA, 16 C.F.R. § 312.5; and
15 d. Failing to establish and maintain reasonable procedures to protect the
16 confidentiality, security, and integrity of Personal Information collected from
17 children under 13, in violation of Section 312.8 of COPPA, 16 C.F.R. § 312.8.

18 302. Violations of COPPA and the accompanying FTC regulations "shall be treated as a
19 violation of a rule defining an unfair ... act or practice prescribed under 15 U.S.C. § 57a(a)(1)(B)." 15
20 U.S.C. § 6502(c). These rules define unfair acts or practices in or affecting commerce within the meaning
21 of 15 U.S.C. § 45(a)(1), which is the model for the various consumer protection statutes in the several
22 states, including the Fla. Stat. Ann. § 501.201, *et seq.*⁴⁸

23 303. Accordingly, Defendants engaged in unfair and unlawful trade acts or practices in
24 violation of Fla. Stat. Ann. § 501.204, *et seq.*, which is modeled after, proscribes the same conduct as,
25 and gives deference to the definitions of the FTC Act.

26 _____
27
28 ⁴⁸ See 16 C.F.R. § 312.1 (COPPA "prohibits unfair or deceptive acts or practices in connection with the
collection, use, and/or disclosure or personal information from and about children on the internet.").

1 304. Defendants' conduct is unfair, immoral, unethical, oppressive, unscrupulous and
2 substantially injurious to consumers, and there are no greater countervailing benefits to consumers or
3 competition. Further, A.C. and members of the Florida Class could not have reasonably avoided injury
4 because Defendants each took advantage of the lack of knowledge, ability, experience, and/or capacity
5 of consumers—in this case children under 13—to their detriment.

6 305. Defendants willfully engaged in the unfair and unlawful acts described herein and knew
7 or recklessly disregarded the fact that they violated Fla. Stat. Ann. § 501.204, *et seq.*

8 306. A.C. and members of the Florida Class were harmed by Defendants' practices described
9 herein, which were a substantial factor and caused injury in fact and actual damages to A.C. and members
10 of the Florida Class.

11 307. As a direct and proximate result of Defendants' unfair and unlawful acts and practices in
12 violation of Fla. Stat. Ann. § 501.204, *et seq.*, A.C. and members of the Florida Class have suffered and
13 will continue to suffer an ascertainable loss of money or property, real or personal, and monetary and
14 non-monetary damages, as described herein, including, inter alia, the loss of the value and/or
15 diminishment in value of their Personal Information and the loss of the ability to control the use of their
16 Personal Information, which allowed Defendants to profit at the expense of A.C. and members of the
17 Florida Class.

18 308. As outlined herein, there is tangible value in A.C. and members of the Florida Class's
19 Personal Information. A.C. and members of the Florida Class have lost the opportunity to receive value
20 in exchange for their Personal Information.

21 309. Defendants' monetization of A.C. and members of the Florida Class's Personal
22 Information demonstrates that there is a market for their Personal Information.

23 310. A.C. and members of the Florida Class's Personal Information is now in the possession
24 of Defendants, who have used and will use it for their financial gain.

25 311. Defendants' retention of A.C. and members of the Florida class's Personal Information
26 presents a continuing risk to them as well as the general public. A.C. and members of the Florida Class
27 seek relief for the injuries they have suffered as a result of Defendants' unfair and unlawful acts and
28 practices, as provided by Fla. Stat. Ann. § 501.204, *et seq.* and applicable law, including all actual

1 damages and attorneys' fees and costs, treble damages, statutory damages, and restitution, as well as an
 2 injunction requiring Defendants to each permanently delete, destroy or otherwise sequester the Personal
 3 Information collected without parental consent, requiring Defendants to provide a complete audit and
 4 accounting of the uses of the Personal Information by them and any other third parties, and other
 5 appropriate injunctive and/or declaratory relief.

6 **Claim 9**

7 **FLORIDA UNJUST ENRICHMENT** 8 **(Against All Defendants on behalf of Plaintiff A.C. and the Florida Class)**

9 312. Plaintiff A.C. and members of the Florida Class re-allege the foregoing allegations as if
 10 fully set forth herein.

11 313. By virtue of the unlawful and unfair conduct alleged herein, Defendants have each realized
 12 millions of dollars in revenue from their collection and use of the Personal Information of A.C. and
 13 Florida Class members through behavioral advertising and commercialization purposes derived from that
 14 Personal Information.

15 314. Defendants' ill-gotten gains were monetary benefits conferred upon Defendants by A.C.
 16 and members of the Florida Class. It would be inequitable and unjust to permit any of the Defendants to
 17 retain the economic benefits they have obtained through advertising and commercialization derived from
 18 the Personal Information of A.C. and members of the Florida Class.

19 315. Defendants will be unjustly enriched if they are permitted to retain the economic benefits
 20 conferred upon them by A.C. and members of the Florida Class through their unlawful, unfair,
 21 unauthorized, and impermissible use of the Personal Information A.C. and members of the Florida Class,
 22 and allowing Defendants to retain the profits from their unlawful, unfair, unauthorized, and impermissible
 23 use of the Personal Information of A.C. and members of the Florida Class would be unjust and contrary
 24 to public policy.

25 316. A.C. and members of the Florida class are therefore entitled to recover the amounts
 26 realized by each of the Defendants at the expense of A.C. and members of the Florida Class.

27 317. A.C. and members of the Florida Class do not seek recovery in this claim for their own
 28 economic harm and have no adequate remedy at law that would divest Defendants of their ill-gotten and

1 unjust profits. To the extent that money damages, if available, would constitute an adequate remedy at
 2 law barring recovery under this claim, A.C. and members of the Florida Class assert their claim for non-
 3 restitutionary disgorgement as an alternative remedy pending a final determination of the availability of
 4 a remedy at law.

5 318. A.C. and members of the Florida Class are entitled to non-restitutionary disgorgement of
 6 each Defendant's ill-gotten gains, and/or the imposition of a constructive trust to recover the amount of
 7 each Defendant's ill-gotten gains.

8 **PRAYER FOR RELIEF**

9 WHEREFORE, Plaintiffs, individually and on behalf of themselves and the proposed Classes,
 10 respectfully request relief as follows:

- 11 A. An order certifying this action as a class action, and certifying the Classes defined herein,
 12 designating Plaintiffs, as described above, as the representatives of the respective Classes
 13 defined herein, and appointing Plaintiffs' counsel as counsel for the Classes;
- 14 B. An order declaring that Defendants' actions, as described above constitute: (i) breaches
 15 of the common law claim of intrusion upon seclusion as to the intrusion upon seclusion
 16 claims set forth above; (ii) violations of the state consumer protection statutes set forth
 17 above; (iii) a violation of the right to privacy under the California Constitution, Article I,
 18 Section 1; and (iv) that Defendants were unjustly enriched as a result of their actions.
- 19 C. A judgment awarding Plaintiffs and the members of the Classes appropriate relief,
 20 including actual, compensatory, and/or statutory damages, and punitive damages (as
 21 permitted by law), in an amount to be determined at trial;
- 22 D. A judgment awarding any and all equitable, injunctive, and declaratory relief as may be
 23 appropriate, including orders of disgorgement of Defendants' unlawful gains, and
 24 restitution;
- 25 E. A judgment awarding injunctive relief as set forth above, non-restitutionary
 26 disgorgement of profits and unlawful gains, and such other equitable relief as the Court
 27 may deem proper;
 28

- 1 F. A judgment awarding all costs, including experts' fees, attorneys' fees, and the costs of
2 prosecuting this action, and other relief as permitted by law;
3 G. Pre-judgment and post-judgment interest, as permitted by law; and
4 H. Grant such other legal and equitable relief as the Court may deem appropriate.

5 **DEMAND FOR JURY TRIAL**

6 Plaintiffs demand a trial by jury for all issues so triable.
7

8 Dated: August 9, 2024

Respectfully submitted,

9 /s/ Patrick Carey

10 Patrick Carey, (Bar No. 308623)
Mark Todzo, (Bar No. 168389)
LEXINGTON LAW GROUP, LLP
503 Divisadero Street
San Francisco, California 94105
Telephone: (415) 913-7800
pcarey@lexlawgroup.com
mtodzo@lexlawgroup.com

15 /s/ David S. Golub

16 **SILVER GOLUB & TEITELL LLP**
David S. Golub (*pro hac vice forthcoming*)
Steven Bloch (*pro hac vice forthcoming*)
Ian W. Sloss (*pro hac vice forthcoming*)
Jennifer Sclar (*pro hac vice forthcoming*)
John Seredynski (*pro hac vice forthcoming*)
One Landmark Square, 15th Floor
Stamford, CT 06901
Telephone: (203) 325-4491
Facsimile: (203) 325-3769
dgolub@sgtlaw.com
sbloch@sgtlaw.com
isloss@sgtlaw.com
jsclar@sgtlaw.com
jseredynski@sgtlaw.com

25 *Attorneys for Plaintiffs*
26 *and the Proposed Classes*
27
28